IBSCO

System Security Plan

17711 Telge Road
Cypress, TX 77429
(800) 231-6480

https://www.ibsco.com/



TESSERACT™
Compiled by Ardalyst
www.ardalyst.com

Disclaimers and Disclosures

This document is developed based on information provided by the Organization Seeking Certification (OSC) ("you", "your") regarding the classification and flow of CUI in your organization and the systems you use (or will use) in your end-state configuration. Their accuracy is dependent on the information you provided. The responsibility for identifying and designating CUI rests solely on you. Nothing in this document should be construed as legal advice. Ardalyst does not determine, interpret, or classify what constitutes Controlled Unclassified Information (CUI) or derivative CUI within your environment. For any determinations regarding CUI, derivative CUI, or related regulatory interpretations, you should consult qualified legal counsel.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

System Security Plan (SSP) Approval

The policies contained herein are approved for immediate implementation and are authorized until replaced. This Cybersecurity Program is governed by DFARS 252.204-7012, 252.204-7019, 252.204-7020, and 252.204-7021, including the guidance provided in NIST SP 800-171, the Cybersecurity Maturity Model Level 2 Certification, the Cybersecurity Maturity Model Level 2 Scoping Guide, and the Cybersecurity Maturity Model Certification Level 2 Assessment Guides. Additional guidelines, if relevant, are noted in each policy.

Signed:

Richard Scroggins

Signature

Richard Scroggins

Printed Name

Technology Manager

Title

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Revision History

CA.L2-3.12.4[g,h]

This document is updated annually at a minimum.

Version Number	Date Last Completed	Notes	Date Next Due
1.0	2025-08-20	Initial Document	2026-08-20
1.1	2026-01-14	Minor Update	2027-01-14
2.0	2026-08-27	Program Update	2027-08-27

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

System Boundary and Scope

CA.L2-3.12.4[b]

The system boundary and scope is defined below. For more details regarding the scope of the system and the flow of CUI through the system, please reference the Scope Enclave and CUI Flow Diagram.

The GCC-H environment contains a suite of productivity and security tools. The boundary around the cloud environment is established via zero-trust identity authentication and data controls. The environment hosts endpoints which can be accessed via TLS 1.2 FIPS-encrypted connections. Inside the environment are a variety of security and productivity tools.

Qualys agents are deployed to end-points and the cloud-based management software is FedRAMP approved.

Azure Virtual desktops exist within the Cloud System boundary and are protected by their own host-based Windows firewalls. They also restrict connectivity to the out-of-scope endpoints used to access them, creating a boundary between the AVD and the accessing endpoint. Connections are established using TLS 1.2 FIPS-validated encrypted tunnels.

Win 365 Desktop-as-a-Service endpoints exist inside the cloud system boundary and are configured to block connections to the out-of-scope devices, providing a boundary between them. They are accessed using FIPS-validated TLS 1.2 encrypted tunnels.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

System Environment of Operation

CA.L2-3.12.4[c]

The system environment of operation is defined below. The environment of operation is defined as the "physical surroundings in which an information system processes, stores, and transmits information. "(CMMC L2 Assessment Guide, v2.13, p. 209)

Cloud only environments significantly mitigate risk by removing the presence of facilities storing sensitive data and media containing sensitive data. Users can access the enclave from anywhere; all access locations are considered out of scope as they do not have any physical CUI media contained within them.

Physical endpoints used to access the cloud are Out of Scope Assets as defined in § 32 CFR 170.19 (c)(1) - Table 3 “CMMC Level 2 Asset Categories and Associated Requirements”, under the asset description “An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset.”

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

External Connection

AC.L2-3.1.20[a,b]; CA.L2-3.12.4[f]

The connections and relationships to external systems (other systems and networks), and their use, are identified in the table below. The connections and relationships to other systems and networks are defined as "description of related, dependent, and interconnected systems" (CMMC L2 Assessment Guide, v2.13, p. 210)

External System	Purpose	Authorized for CUI
Ardalyst <-> Qualys	Patch management solution for managed endpoints	False
Ardalyst -> Keeper	Password Management	False
IBSCO <-> Customer Portals	Various customer portals are used to download and upload CUI	True
IBSCO <-> M365 GCC-H	The GCC-H environment contains a suite of productivity and security tools.	True
IBSCO -> Ardalyst Support Portal	The Ardalyst Support Portal is used for managing cases.	False

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Role Definitions

AT.L2-3.2.2[a]

Information security-related duties, roles, and responsibilities are defined below:

Authorized Publication Reviewer: Authorized Publication Reviewers perform publication review both before and after information is disseminated publicly to ensure that it does not contain any sensitive data.

Authorized Publisher: Authorized Publishers are employees that are authorized to write material to be disseminated publicly and must request reviews from an Authorized Publication Reviewer before dissemination.

Authorized User: Authorized Users are any personnel who are authorized to use the system and/or access the physical environment described in this SSP and are responsible for following policies and procedures when doing so.

Change Management Board Member: The Change Management Board (CMB) performs required duties to determine system baselines and make decisions regarding changes in approved systems, software, and configurations. Members of the Change Management Board who are not serving other roles in the Tesseract Program are frequently business decision makers who weigh in on issues of budget and applicability of system changes to business objectives.

Cloud Service Provider: The Cloud Service Provider is responsible for meeting the obligations laid out in their FedRAMP accreditation.

Cybersecurity Program Director: The Program Director is responsible, on the Program level, for the success of the program and responsible for providing oversight for day-to-day operations. The Director is also accountable for individual policies unless otherwise specified. The Program Director is always a member of the CMB. Common titles for personnel fulfilling the Program Director role are Chief Information Officer, Chief Technical Officer, and Chief Information Security Officer.

Defend Team: Team members implement policies and execute practices to monitor for anomalous events and potential indications of compromise. This includes log monitoring, responding to alerts, incorporating threat intelligence, performing periodic tests of the system, and reporting events to the Incident Response Team for disposition.

Escalation Support Team: The Support team responds to user issues, returns systems to baseline if they are non-performant, and assists the Operate Team in configuring and administering the system, with an emphasis on endpoints.

Govern Team: Govern resource(s) facilitate CMB meetings regarding policies and practices, document policy and practices except as specified in the RASCI for each policy, support the development of practices that meet policy standards, and advise the Program Director on matters of policy and practices.

Harden Team: Team members implement policies and execute practices to reduce the attack surface area of your systems. This includes configuring baselines, deploying patches, and advising the Change Management Board on questions of configuration changes in the environment.

Human Resources Team: The Human Resources Team performs background checks and other personnel management actions, including onboarding and offboarding.

Incident Response Team: The Incident Response Team is responsible for reviewing events reported by Cyber Operations resources to determine if they are incidents and execute the Incident Response Plan. Team members who are not serving in other roles in the Tesseract Program are typically assigned to the team responding to a specific event and include members of business who are responsible for relationships with the vendors or customers that are affected by the security event, and human resources members who assist with the implementation of any legal or disciplinary action involving employees.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Operate Team: Operate Team members assist the Harden team in configuring and administering the environment.

Privileged User: Most of the roles listed will have some sort of privileged function in the organization, which may come with a privileged account. Organizations should consider if there are other privileged functions that they wish to assign to a group of users (such as Department Managers) or even to allow most users to perform a privileged function. The most common example of allowing users a privileged function is allowing sophisticated users (in a technology or engineering company) the ability to administer their own endpoints.

System Administrator: System Administrators are responsible for managing the ongoing use of the system. This includes activities such as adding and removing user accounts, managing user's enrollment in RBAC groups, and adding or removing approved software from systems where regular users are not permitted to do so.

System Deployer: System Deployers are responsible for configuring systems according to a predetermined baseline configuration. This includes activities such as activation of a system, deployment of pre-existing baseline scripts, or manual configuration of a system according to system configuration documentation.

System Designer: System Designers are responsible for the engineering and documentation of the configuration of systems. This includes activities such as analyzing the framework requirements that apply to a system, analyzing a system's capabilities and functionalities in relationship to meeting those requirements, developing and testing baselines for systems, and documenting a standard for deployment.

System Maintainer: Responsible for patching the system, and returning the system to baseline

System Security Analyst: System Security Analysts are responsible for the monitoring of a system for threats or unauthorized use. This includes activities such as reviewing logs and alerts, investigating alerts to determine their significance, conducting remediation activities, and creating cases for Suspected Threat Events.

Technical Lead: The Program Technical Lead is responsible, on the Program level, for advising the Program Director on technical issues, including product selection, configuration, testing and acceptance. Common titles for personnel fulfilling the Program Technical Lead role are Chief Information Security Officer, Chief Technical Officer, and Vice President or Director of Information Technology.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Role Assignments

AT.L2-3.2.2[b]

Information security-related duties, roles and responsibilities are assigned to the designated personnel below:

Role	Assignee	Title	Email
Lead Executive	Richard Scroggins	Technology Manager	richard.scroggins@ibsco.com
Cybersecurity Program Director	Richard Scroggins	Technology Manager	richard.scroggins@ibsco.com
Technical Lead	Richard Scroggins	Technology Manager	richard.scroggins@ibsco.com
Change Management Board Member	Mike Ellsmore		mike.ellsmore@ibsco.com
Incident Response Team	Ardalyst Personnel	Ardalyst Personnel	support@ardalyst.com
	Richard Scroggins	Technology Manager	richard.scroggins@ibsco.com
Govern Team	Ardalyst Personnel	Ardalyst Personnel	support@ardalyst.com
Harden Team	Ardalyst Personnel	Ardalyst Personnel	support@ardalyst.com
Defend Team	Ardalyst Personnel	Ardalyst Personnel	support@ardalyst.com

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Method of Security Requirement Implementation

CA.L2-3.12.4[h]

The methods of security requirement implementation are described and documented below. These descriptions include indicating which security requirements are met via inheritance and which are rendered non-applicable by policy

Practice Code		Practice Name
AC.L2-3.1.1		Authorized Access Control
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Procedure Summary

[a]	The Human Resources Team identifies personnel authorized for system access in the User, Process, and Asset Inventory.
[b]	The Technical Lead identifies authorized service principals in the User, Process, and Asset Inventory.
[c]	The Technical Lead identifies authorized devices in the User, Process, and Asset Inventory.
[d]	The System Deployer configures the system such that system access is limited to authorized users according to the System Baseline Standard.
[e]	The System Deployer configures the system such that system access is limited to authorized service principals according to the System Baseline Standard.
[f]	The System Deployer configures the system such that system access is limited to authorized devices according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.1[a]	Implemented

Assessment Objective

Authorized users are identified

Program Procedure

The Human Resources Team identifies personnel authorized for system access in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Human Resources Team	Govern Team Human Resources Team Operate Team

Process Summary

- The Govern Team documents the policy for authorized access in the Authorized Access Control Section in the 3.1 Access Control Policy.
- The Human Resources Team identifies personnel authorized.
- The Human Resources Team opens an Identity and Access Management Case for personnel additions or removals.
- The Operate Team documents additions or removals of authorized personnel in the User, Process, and Asset Inventory.
- The Operate Team transfers the Identity and Access Management Case to the System Administrator for the creation or disabling of user accounts.

Process Evidence

Authorized Access Control Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

Identity and Access Management Case
- support.ardalyst.com

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.1[b]	Implemented

Assessment Objective

Processes acting on behalf of authorized users are identified

Program Procedure

The Technical Lead identifies authorized service principals in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team Operate Team Technical Lead

Process Summary

- The Govern Team documents the policy for authorized access in the Authorized Access Control Section in the 3.1 Access Control Policy.
- The Technical Lead identifies authorized service principal accounts.
- The Technical Lead opens an Identity and Access Management Case for service principal additions or removals.
- The Operate Team documents the authorization or deauthorization of service principals in the User, Process, and Asset Inventory.
- The Operate Team transfers the Identity and Access Management Case to the System Administrator for the creation or disabling of service principals.

Process Evidence

Authorized Access Control Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

Identity and Access Management Case
- support.ardalyst.com

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.1[c]	Implemented

Assessment Objective

Devices (and other systems) authorized to connect to the system are identified

Program Procedure

The Technical Lead identifies authorized devices in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team Operate Team Technical Lead

Process Summary

- The Govern Team documents the policy for authorized access in the Authorized Access Control Section in the 3.1 Access Control Policy.
- The Technical Lead identifies authorized devices.
- The Technical Lead opens an Identity and Access Management Case for device additions and removals.
- The Operate Team documents authorized devices in the User, Process, and Asset Inventory.
- The Operate Team transfers the Identity and Access Management Case to the System Administrator for device additions and removals.

Process Evidence

Authorized Access Control Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

Identity and Access Management Case
- support.ardalyst.com

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.1[d]	Implemented

Assessment Objective

System access is limited to authorized users

Program Procedure

The System Deployer configures the system such that system access is limited to authorized users according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Multifactor Authentication Methods in the Entra Portal

Win 10/11 AVD

- Configure "CFG-DisableGuestAccount-INT" to disable the built-in Guest account on Windows devices.
- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure "CFG-DisableGuestAccount-INT" to disable the built-in Guest account on Windows devices.
- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

CFG-DisableGuestAccount-INT
- Intune > Devices > Manage Devices > Configuration

CFG-DisallowNullSessions-INT
- Intune > Devices > Manage Devices > Configuration

Entra Authentication Methods Screenshot
- Entra Portal > Protection > Authentication Methods > Manage > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.1[e]	Implemented

Assessment Objective

System access is limited to processes acting on behalf of authorized users

Program Procedure

The System Deployer configures the system such that system access is limited to authorized service principals according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Client Secrets for Service Principals

Win 10/11 AVD

- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares

Win 10/11 Win365

- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares

Configuration Evidence

CFG-DisallowNullSessions-INT

- Intune > Devices > Manage Devices > Configuration

Example App Registration Client Secret

- Azure > App Registrations > Example App > Manage > Certificates and Secrets > Client Secrets

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.1[f]	Implemented

Assessment Objective

System access is limited to authorized devices (including other systems)

Program Procedure

The System Deployer configures the system such that system access is limited to authorized devices according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Conditional Access Policy CAP-RequireMFADeviceEnrollment-EID to require multifactor authentication for device enrollment
- Configure Multifactor Authentication Methods in the Entra Portal

Win 10/11 AVD

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Conditional Access Policy CAP-RequireWorkstationComplianceRichClientAccess-EID to require that workstations accessing through a rich client meet the device compliance policies
- Configure Device Cleanup Rule DCU-DeviceCleanUp-INT to remove devices after 30 days without check-in.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Conditional Access Policy CAP-RequireWorkstationComplianceRichClientAccess-EID to require that workstations accessing through a rich client meet the device compliance policies
- Configure Device Cleanup Rule DCU-DeviceCleanUp-INT to remove devices after 30 days without check-in.

Configuration Evidence

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireMFADeviceEnrollment-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireWorkstationComplianceRichClientAccess-EID
- Entra Admin Portal > Security > Conditional Access

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

DCU-DeviceCleanUp-INT

- Intune > Home > Devices > Device Clean-Up Rules > Create

Entra Authentication Methods Screenshot

- Entra Portal > Protection > Authentication Methods > Manage > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.2		Transaction and Function Control
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Procedure Summary

[a]	The System Designer defines permitted transactions and functions in the System Catalog.
[b]	The System Deployer configures the system to limit the transactions and functions for authorized users to the defined types according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.2[a]	Implemented

Assessment Objective

The types of transactions and functions that authorized users are permitted to execute are defined

Program Procedure

The System Designer defines permitted transactions and functions in the System Catalog.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Administrator System Designer

Process Summary

- The Govern Team documents the requirements for transaction and functions in the Transactions and Functions Control Section in the 3.1 Access Control Policy.
- The System Designer develops the configuration for permitted transactions and functions.
- The System Designer documents the configuration for permitted transactions and functions in the System Catalog.
- The System Administrator assigns privileged functions in the system, and documents privileged function assignments in the User, Process, and Asset Inventory.

Process Evidence

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

Transactions and Functions Control Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.2[b]	Implemented

Assessment Objective

System access is limited to the defined types of transactions and functions for authorized users

Program Procedure

The System Deployer configures the system to limit the transactions and functions for authorized users to the defined types according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Create "GRP-AllUsers-EID" dynamic group for MAM-WE policies in Intune
- Create "GRP-NonPrivUsers-EID" dynamic group to use with conditional access policies
- Privileged functions are not assigned to non-privileged users.

Win 10/11 AVD

- Admins assigned to the “Virtual Machine Administrator Login” Role may perform local admin tasks on the AVD by default
- Assign Required RBAC Permissions to the subscription so the AVD can start on connect.
- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares
- Configure Dynamic Device Security Group "GRP-AllAVDs-EID" to include only Azure Virtual Desktops and Azure Virtual Machines for device management
- Configure the group "GRP-ArdalystHardenPIM-EID" with the role "Microsoft Entra Joined Device Local Administrator" role. These administrators cannot access devices without first using multifactor authentication through the tenant.
- Intune automatically adds Global Administrators, and privileged accounts with the "Microsoft Entra Joined Device Local Administrator" role to the local administrators group in Entra AD joined devices by default.
- Users assigned to the “Virtual Machine User Login” RBAC Role may sign and use the AVD, but may not use local admin permissions by default

Win 10/11 Win365

- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares
- Configure CFG-ReplaceLocalAdmin-INT in Microsoft Intune to remove local administrator rights from users, and replace with select admins from Entra.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

- Configure the group "GRP-ArdalystHardenPIM-EID" with the role "Microsoft Entra Joined Device Local Administrator" role. These administrators cannot access devices without first using multifactor authentication through the tenant.
- Intune automatically adds Global Administrators, and privileged accounts with the "Microsoft Entra Joined Device Local Administrator" role to the local administrators group in Entra AD joined devices by default.

Configuration Evidence

"GRP-AllUsers-EID" Group
- Azure Admin Console -> Entra ID -> Groups

"GRP-NonPrivUsers-EID" Group
- Azure Admin Console -> Entra ID -> Groups

AVD RBAC Roles
- Azure > Resource Groups > [AVD Resource Group] > [Example AVD] > Access Control (IAM) > Role Assignments

CFG-DisallowNullSessions-INT
- Intune > Devices > Manage Devices > Configuration

CFG-ReplaceLocalAdmin-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

GRP-AllAVDs-EID
- Azure Admin Console -> Entra ID -> Groups

GRP-ArdalystHardenPIM-EID
- Azure > Entra > Groups

Microsoft Entra Joined Device Local Administrator Article
- https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#microsoft-entra-joined-device-local-administrator

Non-privileged account roles
- Entra ID > Users > [non-privileged user] > Assigned Roles

Roles Defined in Entra PIM
- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

Start VM on Connect RBAC Permission
- Azure > Subscription > Access Control (IAM) > role assignments

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.3		Control CUI Flow
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Control the flow of CUI in accordance with approved authorizations.

Procedure Summary

[a]	The Govern Team defines policies to control the flow of CUI in the CUI Flow in the 3.1 Access Control Policy.
[b]	The Govern Team defines methods and enforcement mechanisms for controlling the flow of CUI for each system configuration and documents in the Scope Enclave and CUI Flow Diagram.
[c]	The Cybersecurity Program Director identifies sources and destinations of CUI, and documents in the Scope Enclave and CUI Flow Diagram.
[d]	The Harden Team defines authorizations for each source and destination within the system and between interconnected systems in the Scope Enclave and CUI Flow Diagram.
[e]	The System Deployer enforces approved authorizations for controlling CUI through baseline configurations related to controlling the flow of CUI.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.3[a]	Implemented

Assessment Objective

Information flow control policies are defined

Program Procedure

The Govern Team defines policies to control the flow of CUI in the CUI Flow in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Govern Team defines information control flow policies in the CUI Flow in the 3.1 Access Control Policy.
- The Govern Team documents information control flow policies in the CUI Flow in the 3.1 Access Control Policy.
- The Govern Team defines policies to control the flow of CUI in the CUI Flow in the 3.1 Access Control Policy.
- The Cybersecurity Program Director identifies users authorized to handle CUI.
- The Cybersecurity Program Director identifies systems that are scoped as CUI assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and Out of Scope Assets.
- The Cybersecurity Program Director identifies locations where CUI is authorized to be stored.
- The Cybersecurity Program Director identifies locations where CUI is authorized to be accessed remotely.
- The Cybersecurity Program Director identifies type of media (paper, digital, portable, or backup) that contain CUI.
- The Govern Team documents users authorized to handle CUI in the User, Process, and Asset Inventory.
- The Govern Team documents systems that are scoped as CUI assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and Out of Scope Assets in the Scope Enclave and CUI Flow Diagram.
- The Govern Team documents locations where CUI is authorized to be stored in the Scope Enclave and CUI Flow Diagram.
- The Govern Team documents locations where CUI is authorized to be accessed remotely in the Scope Enclave and CUI Flow Diagram.
- The Govern Team documents type of media (paper, digital, portable, or backup) that contain CUI in the Scope Enclave and CUI Flow Diagram.

Process Evidence

CUI Flow
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.3[b]	Implemented

Assessment Objective

Methods and enforcement mechanisms for controlling the flow of CUI are defined

Program Procedure

The Govern Team defines methods and enforcement mechanisms for controlling the flow of CUI for each system configuration and documents in the Scope Enclave and CUI Flow Diagram.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team defines methods and enforcement mechanisms for controlling the flow of CUI for each system configuration and documents in the Scope Enclave and CUI Flow Diagram.

Process Evidence

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.3[c]	Implemented

Assessment Objective

Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified

Program Procedure

The Cybersecurity Program Director identifies sources and destinations of CUI, and documents in the Scope Enclave and CUI Flow Diagram.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team Operate Team

Process Summary

- The Cybersecurity Program Director identifies sources of CUI.
- The Govern Team documents sources of CUI in the Scope Enclave and CUI Flow Diagram.
- The Operate Team documents authorized sources of CUI in the User, Process, and Asset Inventory as an approved source.
- The Cybersecurity Program Director identifies destinations of CUI.
- The Govern Team documents destinations of CUI in the Scope Enclave and CUI Flow Diagram.
- The Operate Team documents authorized destinations of CUI in the User, Process, and Asset Inventory as an approved destination.

Process Evidence

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.3[d]	Implemented

Assessment Objective

Authorizations for controlling the flow of CUI are defined

Program Procedure

The Harden Team defines authorizations for each source and destination within the system and between interconnected systems in the Scope Enclave and CUI Flow Diagram.

Procedure Type	Responsible Role	Supporting Roles
Process	Harden Team	Cybersecurity Program Director Govern Team

Process Summary

- The Govern Team documents that the Cybersecurity Program Director is responsible for authorizing sources and destinations for CUI and documents in the CUI Flow section of the 3.1 Access Control Policy.
- The Cybersecurity Program Director reviews the completed Scope Enclave and CUI Flow Diagram.
- The Cybersecurity Program Director accepts completed Scope Enclave and CUI Flow Diagram.

Process Evidence

CUI Flow
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.3[e]	Implemented

Assessment Objective

Approved authorizations for controlling the flow of CUI are enforced

Program Procedure

The System Deployer enforces approved authorizations for controlling CUI through baseline configurations related to controlling the flow of CUI.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure CAP-BlockBrowserUnmanagedDeviceV1.1-EID to block browser access from unmanaged devices
- Configure Conditional Access Policy CAP-BlockUntrustedLocations-EID to block connections from untrusted locations
- Microsoft provides an email encryption tool by default.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 AVD

- Configure CFG-BlockAVDClipboardRedirection-INT to block clipboard redirection to client endpoints from AVD sessions
- Configure CFG-BlockAVDDriveRedirection-INT to block drive redirection to client endpoints from AVD sessions.
- Configure CFG-BlockAVDPrinterRedirection-INT to block printer redirection to client endpoints from AVD sessions
- Configure CFG-BlockAVDUSBDriveRedirection-INT to block AVD drive redirection to client endpoints from AVD sessions
- Configure CFG-BlockClientScreenShotOnVirtualDesktopConnections-INT to disable screenshots of virtual machine sessions on client devices
- Microsoft provides an email encryption tool by default.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Configure CFG-BlockClientScreenShotOnVirtualDesktopConnections-INT to disable screenshots of virtual machine sessions on client devices
- Configure CFG-BlockW365ClipboardRedirection-INT to block clipboard redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365DriveRedirection-INT to block drive redirection to client endpoints from W365 sessions

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- Configure CFG-BlockW365PrinterRedirection-INT to block printer redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365USBDriveRedirection-INT to block USB drive redirection to client endpoints from W365 sessions
- Microsoft provides an email encryption tool by default.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Configuration Evidence

CAP-BlockBrowserUnmanagedDeviceV1.1-EID
- Entra Admin Portal > Security > Conditional Access

CAP-BlockUntrustedLocations-EID
- Entra Admin Portal > Security > Conditional Access

CFG-BlockAVDClipboardRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDPrinterRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDUSBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockClientScreenShotOnVirtualDesktopConnections-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365ClipboardRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365DriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365PrinterRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365USBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Microsoft Email Encryption Learn Article
- https://learn.microsoft.com/en-us/purview/ome

Technical Reference Details About Encryption Learn Article
- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.4		Separation Of Duties
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Procedure Summary

[a]	The Govern Team defines that managing audit logs and alerts requires separation in the Separation of Duties Section in the 3.1 Access Control Policy.
[b]	The Govern Team assigns the Defend role to individuals in the User, Process, and Asset Inventory.
[c]	The System Administrator assigns audit record management access to Defend individuals and Global Administrators only.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.4[a]	Implemented

Assessment Objective
The duties of individuals requiring separation are defined

Program Procedure
The Govern Team defines that managing audit logs and alerts requires separation in the Separation of Duties Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents that managing audit logs and alerts requires separation in the Separation of Duties Section in the 3.1 Access Control Policy.

Process Evidence

Separation of Duties Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.4[b]	Implemented

Assessment Objective

Responsibilities for duties that require separation are assigned to separate individuals

Program Procedure

The Govern Team assigns the Defend role to individuals in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team assigns the Defend role to individuals in the User, Process, and Asset Inventory.

Process Evidence

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.4[c]	Implemented

Assessment Objective

Access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals

Program Procedure

The System Administrator assigns audit record management access to Defend individuals and Global Administrators only.

Procedure Type	Responsible Role	Supporting Roles
Process	System Administrator	System Administrator System Designer

Process Summary

- The System Designer documents the RBAC roles that allow access to audit logs and alerts in the User, Process, and Asset Inventory.
- The System Administrator assigns the RBAC role to allow audit record management access to Defend Team members.
- The System Administrator grants Global Administrator access to approved personnel in the User, Process, and Asset Inventory.

Process Evidence

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.5		Least Privilege
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Employ the principle of least privilege, including for specific security functions and privileged accounts.

Procedure Summary

[a]	The Technical Lead identifies privileged accounts in the User, Process, and Asset Inventory.
[b]	The Technical Lead assigns job roles to personnel in the User, Process, and Asset Inventory.
[c]	The System Designer identifies privileged functions in the User, Process, and Asset Inventory.
[d]	The Technical Lead authorizes assignment of privileged functions to privileged accounts in the User, Process, and Asset Inventory.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.5[a]	Implemented

Assessment Objective

Privileged accounts are identified

Program Procedure

The Technical Lead identifies privileged accounts in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team Operate Team System Administrator Technical Lead

Process Summary

- The Govern Team documents the requirements for least privilege in the Least Privilege Section in the 3.1 Access Control Policy.
- The Technical Lead identifies privileged accounts.
- The Technical Lead identifies privileged account assignments to personnel.
- The Technical Lead opens an Identity and Access Management Case for privileged account creation, modification, or disabling.
- The Operate Team documents privileged accounts in the User, Process, and Asset Inventory.
- The Operate Team documents privileged account personnel assignments in the User, Process, and Asset Inventory.
- The System Administrator creates, modifies, or disables a privileged account.

Process Evidence

Identity and Access Management Case
- support.ardalyst.com

Least Privilege Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Assessment Objective Identifier	Assessment Objective Status
3.1.5[b]	Implemented

Assessment Objective

Access to privileged accounts is authorized in accordance with the principle of least privilege

Program Procedure

The Technical Lead assigns job roles to personnel in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team Operate Team System Designer Technical Lead

Process Summary

- The Govern Team documents the requirements for least privilege in the Least Privilege Section in the 3.1 Access Control Policy.
- The Technical Lead identifies personnel job roles that necessitate a privileged account.
- The System Designer documents personnel job roles in the User, Process, and Asset Inventory.
- The Technical Lead identifies personnel job role assignments.
- The Technical Lead opens an Identity and Access Management Case for personnel job role assignments and removals.
- The Operate Team documents personnel job role assignments in the User, Process, and Asset Inventory.

Process Evidence

Identity and Access Management Case
- support.ardalyst.com

Least Privilege Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Assessment Objective Identifier	Assessment Objective Status
3.1.5[c]	Implemented

Assessment Objective
Security functions are identified

Program Procedure
The System Designer identifies privileged functions in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	System Designer

Process Summary

- The System Designer identifies privileged functions.
- The System Designer documents privileged functions in the User, Process, and Asset Inventory.

Process Evidence

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.5[d]	Implemented

Assessment Objective

Access to security functions is authorized in accordance with the principle of least privilege

Program Procedure

The Technical Lead authorizes assignment of privileged functions to privileged accounts in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Operate Team System Designer Technical Lead

Process Summary

- The Technical Lead identifies personnel job roles that necessitate privileged functions.
- The System Designer documents personnel job roles in the User, Process, and Asset Inventory.
- The Technical Lead identifies personnel job role assignments.
- The Technical Lead opens an Identity and Access Management Case for personnel job role assignments and removals.
- The Operate Team documents personnel job role assignments in the User, Process, and Asset Inventory.

Process Evidence

Identity and Access Management Case
- support.ardalyst.com

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.6		Non-Privileged Account Use
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Use non-privileged accounts or roles when accessing nonsecurity functions.

Procedure Summary

[a]	The System Designer documents the nonsecurity functions in the Non-Privileged Account Use Section of the 3.1 Access Control Policy.
[b]	The System Deployer configures the system such that users must use non-privileged accounts for nonsecurity functions according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.6[a]	Implemented

Assessment Objective

Nonsecurity functions are identified

Program Procedure

The System Designer documents the nonsecurity functions in the Non-Privileged Account Use Section of the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team

Process Summary

- The Govern Team documents the requirements for nonsecurity functions in the Non-Privileged Account Use Section in the 3.1 Access Control Policy.
- The Govern Team documents the nonsecurity functions in the Non-Privileged Account Use Section.

Process Evidence

Non-Privileged Account Use Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.6[b]	Implemented

Assessment Objective

Users are required to use non-privileged accounts or roles when accessing nonsecurity functions

Program Procedure

The System Deployer configures the system such that users must use non-privileged accounts for nonsecurity functions according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Sentinel Analytic rule SAR-AdminLicenseAlert-SEN event is triggered when admins are assigned licenses
- Privileged functions are not assigned to non-privileged users.

Configuration Evidence

Non-privileged account roles

- Entra ID > Users > [non-privileged user] > Assigned Roles

SAR-AdminLicenseAlert-SEN Screenshot

- Sentinel > Configuration > Analytics

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.7		Privileged Functions
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Procedure Summary

[a]	The Govern Team defines privileged functions and documents in the Privileged Functions Section in the 3.1 Access Control Policy.
[b]	The Govern Team defines non-privileged users and documents in the Privileged Functions Section in the 3.1 Access Control Policy.
[c]	The System Deployer configures the system to prevent non-privileged users from executing privileged functions according to the System Baseline Standard.
[d]	The System Deployer configures the system to capture the execution of privileged functions in audit logs according to System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.7[a]	Implemented

Assessment Objective

Privileged functions are defined

Program Procedure

The Govern Team defines privileged functions and documents in the Privileged Functions Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team System Designer

Process Summary

- The Govern Team defines privileged functions.
- The Govern Team documents the requirements for privileged function execution prevention in the Privileged Functions Section in the 3.1 Access Control Policy.
- The System Designer develops the configuration for privileged function execution prevention.
- The System Designer documents the configuration for privileged function execution prevention in the System Baseline Standard.

Process Evidence

Privileged Functions Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.7[b]	Implemented

Assessment Objective

Non-privileged users are defined

Program Procedure

The Govern Team defines non-privileged users and documents in the Privileged Functions Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team defines non-privileged users.
- The Govern Team documents the definition of non-privileged users in the Privileged Functions Section in the 3.1 Access Control Policy.

Process Evidence

Privileged Functions Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.7[c]	Implemented

Assessment Objective

Non-privileged users are prevented from executing privileged functions

Program Procedure

The System Deployer configures the system to prevent non-privileged users from executing privileged functions according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Privileged functions are not assigned to non-privileged users.

Win 10/11 AVD

- Assign Required RBAC Permissions to the subscription so the AVD can start on connect.

Configuration Evidence

Non-privileged account roles
- Entra ID > Users > [non-privileged user] > Assigned Roles

Roles Defined in Entra PIM
- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

Start VM on Connect RBAC Permission
- Azure > Subscription > Access Control (IAM) > role assignments

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.7[d]	Implemented

Assessment Objective

The execution of privileged functions is captured in audit logs

Program Procedure

The System Deployer configures the system to capture the execution of privileged functions in audit logs according to System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- After connectors are set up, Defender XDR audits all cloud operations by default. Each audit log entry contains a user's immutable objectID that can be used to uniquely trace an individual system user to each action.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default

Win 10/11 AVD

- Assign Required RBAC Permissions to the subscription so the AVD can start on connect.

Configuration Evidence

Microsoft CMMC Additional Controls Learn Article
- https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-additional-controls

Microsoft Defender XDR to Sentinel Connector Learn Article
- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

Start VM on Connect RBAC Permission
- Azure > Subscription > Access Control (IAM) > role assignments

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.8		Unsuccessful Logon Attempts
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Limit unsuccessful logon attempts.

Procedure Summary

[a]	The Govern Team defines a limit of no more than ten (10) logon attempts in the Unsuccessful Logon Attempts Section of the 3.1 Access Control Policy.
[b]	The System Deployer configures the system to limit unsuccessful logon attempts to no more than ten (10) attempts according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.8[a]	Implemented

Assessment Objective

The means of limiting unsuccessful logon attempts is defined

Program Procedure

The Govern Team defines a limit of no more than ten (10) logon attempts in the Unsuccessful Logon Attempts Section of the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team System Designer Technical Lead

Process Summary

- The Technical Lead determines the threshold for the number of unsuccessful logon attempts.
- The Govern Team documents the policy for unsuccessful login attempts in the Unsuccessful Logon Attempts Section of the 3.1 Access Control Policy.
- The System Designer develops the configuration to enforce the number of logon attempts as no more than ten (10) attempts.
- The System Designer documents the configuration to enforce the number of logon attempts as no more than ten (10) attempts in the System Baseline Standard.

Process Evidence

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

Unsuccessful Logon Attempts Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.8[b]	Implemented

Assessment Objective

The defined means of limiting unsuccessful logon attempts is implemented

Program Procedure

The System Deployer configures the system to limit unsuccessful logon attempts to no more than ten (10) attempts according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure the Password Protection settings in Microsoft Entra to enable the maximum number of unsuccessful logon attempts that are allowed to five (5) attempts.

Configuration Evidence

Password Protection

- Entra Portal > Security > Manage > Authentication Methods > Password Protection > Lockout threshold

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.9		Privacy and Security Notices
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Provide privacy and security notices consistent with applicable CUI rules.

Procedure Summary

[a]	The Govern Team documents privacy and security banner in the Privacy and Security Notice Section in the 3.1 Access Control Policy.
[b]	The System Deployer configures the system to display privacy and security notice according to System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.9[a]	Implemented

Assessment Objective

Privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category

Program Procedure

The Govern Team documents privacy and security banner in the Privacy and Security Notice Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team System Designer

Process Summary

- The Cybersecurity Program Director develops privacy and security notices required by CUI-specified rules.
- The Govern Team documents privacy and security notices required by CUI-specified rules in the Privacy and Security Notice Section in the 3.1 Access Control Policy.
- The System Designer develops configurations to display the privacy and security notices.
- The System Designer documents the configuration to display the privacy and security notices required by CUI-specified rules in the System Baseline Standard.

Process Evidence

Privacy and Security Notice Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.9[b]	Implemented

Assessment Objective

Privacy and security notices are displayed

Program Procedure

The System Deployer configures the system to display privacy and security notice according to System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure custom company branding in Entra to display a banner on sign in

Win 10/11 AVD

- Configure CFG-InteractiveLogonBanner-INT to display an interactive banner on device sign in

Win 10/11 Win365

- Configure CFG-InteractiveLogonBanner-INT to display an interactive banner on device sign in

Configuration Evidence

CFG-InteractiveLogonBanner-INT

- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Entra Company Branding

- Azure > Entra ID > Manage > Company Branding > Default Sign-In > Sign-in form

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.10		Session Lock
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

Procedure Summary

[a]	The Govern Team defines the period of inactivity after which the system initiates a session lock and documents in the Session Lock Section in the 3.1 Access Control Policy.
[b]	The System Deployer configures applicable systems to prevent access and viewing of data after no more than sixty (60) minutes of inactivity according to the System Baseline Standard.
[c]	The System Deployer configures applicable systems to conceal previously visible information after no more than sixty (60) minutes of inactivity according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.10[a]	Implemented

Assessment Objective

The period of inactivity after which the system initiates a session lock is defined

Program Procedure

The Govern Team defines the period of inactivity after which the system initiates a session lock and documents in the Session Lock Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team System Designer

Process Summary

- The Cybersecurity Program Director defines the period of inactivity after which the system initiates a session lock on a per-system basis.
- The Govern Team documents the session lock time as no more than sixty (60) minutes in the Session Lock Section in the 3.1 Access Control Policy.
- The System Designer develops the configuration to use session lock with pattern-hiding displays.
- The System Designer documents the configuration to use session lock with pattern-hiding displays in the System Baseline Standard.

Process Evidence

Session Lock Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.10[b]	Implemented

Assessment Objective

Access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity

Program Procedure

The System Deployer configures applicable systems to prevent access and viewing of data after no more than sixty (60) minutes of inactivity according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Idle Session Timeout in the M365 admin center to sign users automatically out of Microsoft 365 web apps after sixty (60) minutes.
- Set the Directory Level Idle Timeout in Azure to sixty (60) minutes.

Win 10/11 AVD

- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes

Win 10/11 Win365

- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes

Configuration Evidence

CFG-DisconnectIdleRemoteSessions-INT

- Go to Intune Admin Center → Devices → Configuration

CFG-RemoveIdleDisconnectedSessions-INT

- Go to Intune Admin Center → Devices → Configuration

Directory Level Idle Timeout

- Azure > Top Right Settings Cog > Signing Out + Notifications > Enable Directory Level Timeout

Idle Session Timeout

- Microsoft Admin Center (portal.office365.us/adminportal) > Settings > Org Settings > Security and Privacy > Idle Session Timeout

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.10[c]	Implemented

Assessment Objective

Previously visible information is concealed via a pattern-hiding display after the defined period of inactivity

Program Procedure

The System Deployer configures applicable systems to conceal previously visible information after no more than sixty (60) minutes of inactivity according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Idle Session Timeout in the M365 admin center to sign users automatically out of Microsoft 365 web apps after sixty (60) minutes.
- Set the Directory Level Idle Timeout in Azure to sixty (60) minutes.

Win 10/11 AVD

- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes

Win 10/11 Win365

- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes

Configuration Evidence

CFG-DisconnectIdleRemoteSessions-INT

- Go to Intune Admin Center → Devices → Configuration

CFG-RemoveIdleDisconnectedSessions-INT

- Go to Intune Admin Center → Devices → Configuration

Directory Level Idle Timeout

- Azure > Top Right Settings Cog > Signing Out + Notifications > Enable Directory Level Timeout

Idle Session Timeout

- Microsoft Admin Center (portal.office365.us/adminportal) > Settings > Org Settings > Security and Privacy > Idle Session Timeout

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.11		Session Termination
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Terminate (automatically) a user session after a defined condition.

Procedure Summary

[a]	The Technical Lead defines conditions requiring a user session to terminate are defined as a period of user inactivity no more than sixty (60) minutes in the Session Termination Section of the 3.1 Access Control Policy.
[b]	The System Deployer configures the system to terminate user sessions under the defined conditions according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.11[a]	Implemented

Assessment Objective

Conditions requiring a user session to terminate are defined

Program Procedure

The Technical Lead defines conditions requiring a user session to terminate are defined as a period of user inactivity no more than sixty (60) minutes in the Session Termination Section of the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team System Designer Technical Lead

Process Summary

- The Technical Lead defines the conditions requiring the termination of a user session.
- The Govern Team documents the conditions requiring a user session to terminate are defined as a period of user inactivity no more than sixty (60) minutes in the Session Termination Section of the 3.1 Access Control Policy.
- The System Designer develops the configurations for the user session to terminate under the defined conditions.
- The System Designer documents the configurations for the user session to terminate under the defined conditions in the System Baseline Standard.

Process Evidence

Session Termination Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.11[b]	Implemented

Assessment Objective

A user session is automatically terminated after any of the defined conditions occur

Program Procedure

The System Deployer configures the system to terminate user sessions under the defined conditions according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Idle Session Timeout in the M365 admin center to sign users automatically out of Microsoft 365 web apps after sixty (60) minutes.
- Set the Directory Level Idle Timeout in Azure to sixty (60) minutes.

Win 10/11 AVD

- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes

Win 10/11 Win365

- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes

Configuration Evidence

CFG-DisconnectIdleRemoteSessions-INT

- Go to Intune Admin Center → Devices → Configuration

CFG-RemoveIdleDisconnectedSessions-INT

- Go to Intune Admin Center → Devices → Configuration

Directory Level Idle Timeout

- Azure > Top Right Settings Cog > Signing Out + Notifications > Enable Directory Level Timeout

Idle Session Timeout

- Microsoft Admin Center (portal.office365.us/adminportal) > Settings > Org Settings > Security and Privacy > Idle Session Timeout

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.12		Control Remote Access
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Monitor and control remote access sessions.

Procedure Summary

[a]	The Govern Team permits remote access in the Controlling Remote Access Section in the 3.1 Access Control Policy.
[b]	The System Designer documents the types of permitted remote access in the System Catalog.
[c]	The System Deployer configures systems such that remote access sessions are controlled according to the System Baseline Standard.
[d]	The System Security Analyst monitors remote access sessions.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.12[a]	Implemented

Assessment Objective
Remote access sessions are permitted

Program Procedure
The Govern Team permits remote access in the Controlling Remote Access Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if remote access is permitted.
- The Govern Team documents that remote access is permitted in the Controlling Remote Access Section in the 3.1 Access Control Policy.

Process Evidence

Controlling Remote Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.12[b]	Implemented

Assessment Objective

The types of permitted remote access are identified

Program Procedure

The System Designer documents the types of permitted remote access in the System Catalog.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	System Designer

Process Summary

- The System Designer documents the types of permitted remote access in the System Catalog.

Process Evidence

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.12[c]	Implemented

Assessment Objective

Remote access sessions are controlled

Program Procedure

The System Deployer configures systems such that remote access sessions are controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-BlockLegacyAuthentication-EID to block legacy authentication methods
- Configure Conditional Access Policy CAP-BlockUntrustedLocations-EID to block connections from untrusted locations
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 AVD

- Configure Conditional Access Policy CAP-RequireWorkstationComplianceRichClientAccess-EID to require that workstations accessing through a rich client meet the device compliance policies
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-RequireWorkstationComplianceRichClientAccess-EID to require that workstations accessing through a rich client meet the device compliance policies
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Configuration Evidence

CAP-BlockLegacyAuthentication-EID
- Entra Admin Portal > Security > Conditional Access

CAP-BlockUntrustedLocations-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireWorkstationComplianceRichClientAccess-EID
- Entra Admin Portal > Security > Conditional Access

Technical Reference Details About Encryption Learn Article
- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.12[d]	Implemented

Assessment Objective

Remote access sessions are monitored

Program Procedure

The System Security Analyst monitors remote access sessions.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Configure Microsoft Entra ID data connector to send audit, sign in and non-interactive sign in logs to the Log Analytics Workspace.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default
- Microsoft logs sign-ins by default. Microsoft Sentinel analyzes sign in logs and alerts on suspicious behavior.
- Microsoft Sentinel provides audit reduction and report generation by default

Win 10/11 AVD

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Win 10/11 Win365

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Configuration Evidence

EDR-DeployDefenderConnector-INT
- Intune Portal > Endpoint Security > Endpoint Detection and Response

Microsoft Defender XDR to Sentinel Connector Learn Article
- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

Microsoft Entra ID Log Diagnostic Settings
- Entra ID > Monitoring > Diagnostic settings

Microsoft Sign-In Logs Learn Article
- https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-sign-ins

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.13		Remote Access Confidentiality
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Procedure Summary

[a]	The System Designer documents that cryptographic mechanisms to protect the confidentiality of remote access sessions are identified in the System Baseline Standard.
[b]	The System Deployer configures the system such that cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.13[a]	Implemented

Assessment Objective

Cryptographic mechanisms to protect the confidentiality of remote access sessions are identified

Program Procedure

The System Designer documents that cryptographic mechanisms to protect the confidentiality of remote access sessions are identified in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents that cryptographic mechanisms to protect the confidentiality of remote access sessions are identified in the Remote Access Confidentiality Section in the 3.1 Access Control Policy.
- The System Designer develops the configuration such that cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.
- The System Designer documents the configuration that cryptographic mechanisms to protect the confidentiality of remote access sessions are identified in the System Baseline Standard.

Process Evidence

Remote Access Confidentiality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.13[b]	Implemented

Assessment Objective

Cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented

Program Procedure

The System Deployer configures the system such that cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 AVD

- Configure Intune device configuration policy CFG-EnforceFIPSMode-INT to enforce FIPS compliance on endpoints at the Windows operating system level
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Configure Intune device configuration policy CFG-EnforceFIPSMode-INT to enforce FIPS compliance on endpoints at the Windows operating system level
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Configuration Evidence

CFG-EnforceFIPSMode-INT

- Microsoft Intune Admin Center > Devices > Managed Devices > Configuration > Policies

Technical Reference Details About Encryption Learn Article

- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.14		Remote Access Routing
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Route remote access via managed access control points.

Procedure Summary

[a]	The System Deployer configures the system such that managed access control points are implemented according to the System Baseline Standard.
[b]	The System Deployer configures the system such that remote access is routed through managed access control points according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.14[a]	Implemented

Assessment Objective

Managed access control points are identified and implemented

Program Procedure

The System Deployer configures the system such that managed access control points are implemented according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 AVD

- Configure CFG-BlockAVDClipboardRedirection-INT to block clipboard redirection to client endpoints from AVD sessions
- Configure CFG-BlockAVDDriveRedirection-INT to block drive redirection to client endpoints from AVD sessions.
- Configure CFG-BlockAVDPrinterRedirection-INT to block printer redirection to client endpoints from AVD sessions
- Configure CFG-BlockAVDUSBDriveRedirection-INT to block AVD drive redirection to client endpoints from AVD sessions
- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure CFG-BlockW365ClipboardRedirection-INT to block clipboard redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365DriveRedirection-INT to block drive redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365PrinterRedirection-INT to block printer redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365USBDriveRedirection-INT to block USB drive redirection to client endpoints from W365 sessions

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceConditionalAccessAppControlOnBrowser-EID
- Entra Admin Portal > Security > Conditional Access

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

CFG-BlockAVDClipboardRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDPrinterRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDUSBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365ClipboardRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365DriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365PrinterRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365USBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.14[b]	Implemented

Assessment Objective

Remote access is routed through managed network access control points

Program Procedure

The System Deployer configures the system such that remote access is routed through managed access control points according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.

Win 10/11 AVD

- Configure CFG-BlockAVDClipboardRedirection-INT to block clipboard redirection to client endpoints from AVD sessions
- Configure CFG-BlockAVDDriveRedirection-INT to block drive redirection to client endpoints from AVD sessions.
- Configure CFG-BlockAVDPrinterRedirection-INT to block printer redirection to client endpoints from AVD sessions
- Configure CFG-BlockAVDUSBDriveRedirection-INT to block AVD drive redirection to client endpoints from AVD sessions
- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.

Win 10/11 Win365

- Configure CFG-BlockW365ClipboardRedirection-INT to block clipboard redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365DriveRedirection-INT to block drive redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365PrinterRedirection-INT to block printer redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365USBDriveRedirection-INT to block USB drive redirection to client endpoints from W365 sessions
- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.

Configuration Evidence

CAP-EnforceConditionalAccessAppControlOnBrowser-EID

- Entra Admin Portal > Security > Conditional Access

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

CFG-BlockAVDClipboardRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDPrinterRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDUSBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365ClipboardRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365DriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365PrinterRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365USBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.15		Privileged Remote Access
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Authorize remote execution of privileged commands and remote access to security-relevant information.

Procedure Summary

[a]	The Govern Team identifies that all privileged commands are authorized for remote execution in the Privileged Remote Access Section in the 3.1 Access Control Policy.
[b]	The Govern Team documents security-relevant information authorized to be accessed remotely in the Privileged Remote Access Section in the 3.1 Access Control Policy.
[c]	The Cybersecurity Program Director authorizes execution of privileged commands remotely.
[d]	The Cybersecurity Program Director authorizes the remote access of security-relevant information.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.15[a]	Implemented

Assessment Objective

Privileged commands authorized for remote execution are identified

Program Procedure

The Govern Team identifies that all privileged commands are authorized for remote execution in the Privileged Remote Access Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team identifies that all privileged commands are authorized for remote execution.
- The Govern Team documents that all privileged commands are authorized for remote execution in the Privileged Remote Access Section in the 3.1 Access Control Policy.

Process Evidence

Privileged Remote Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.15[b]	Implemented

Assessment Objective

Security-relevant information authorized to be accessed remotely is identified

Program Procedure

The Govern Team documents security-relevant information authorized to be accessed remotely in the Privileged Remote Access Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team identifies that all security-relevant information is authorized to be accessed remotely.
- The Govern Team documents all security-relevant information authorized to be accessed remotely in the Privileged Remote Access Section in the 3.1 Access Control Policy.

Process Evidence

Privileged Remote Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.15[c]	Implemented

Assessment Objective
The execution of the identified privileged commands via remote access is authorized

Program Procedure
The Cybersecurity Program Director authorizes execution of privileged commands remotely.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director

Process Summary

- The Cybersecurity Program Director accepts the policy to authorize all privileged commands for remote execution.

Process Evidence

Privileged Remote Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.15[d]	Implemented

Assessment Objective
Access to the identified security-relevant information via remote access is authorized

Program Procedure		
The Cybersecurity Program Director authorizes the remote access of security-relevant information.		
Procedure Type	**Responsible Role**	**Supporting Roles**
Process	Cybersecurity Program Director	Cybersecurity Program Director

Process Summary

- The Cybersecurity Program Director accepts the policy to authorize all security-relevant information to be accessed remotely.

Process Evidence

Privileged Remote Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.16		Wireless Access Authorization
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Authorize wireless access prior to allowing such connections.

Procedure Summary

[a]	The Govern Team documents that there are no in scope devices capable of connecting to wireless access points in the Wireless Access Authorization Section in the 3.1 Access Control Policy.
[b]	The Govern Team documents that there are no in scope devices capable of connecting to wireless access points in the Wireless Access Authorization Section in the 3.1 Access Control Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.16[a]	Implemented

Assessment Objective

Wireless access points are identified

Program Procedure

The Govern Team documents that there are no in scope devices capable of connecting to wireless access points in the Wireless Access Authorization Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team Technical Lead

Process Summary

- The Technical Lead determines that there are no in-scope devices capable of connecting to wireless access points.
- The Govern Team documents that there are no in-scope devices capable of connecting to wireless access points in the Wireless Access Authorization Section in the 3.1 Access Control Policy.

Process Evidence

Wireless Access Authorization Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.16[b]	Implemented

Assessment Objective

Wireless access is authorized prior to allowing such connections

Program Procedure

The Govern Team documents that there are no in scope devices capable of connecting to wireless access points in the Wireless Access Authorization Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team Technical Lead

Process Summary

- The Technical Lead determines that there are no in-scope devices capable of connecting to wireless access points.
- The Govern Team documents that there are no in-scope devices capable of connecting to wireless access points in the Wireless Access Authorization Section in the 3.1 Access Control Policy.

Process Evidence

Wireless Access Authorization Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.17		Wireless Access Protection
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Protect wireless access using authentication and encryption.

Procedure Summary

[a]	The Govern Team documents that corporate managed wireless access is not permitted, and all wireless access must be protected by a virtual private network or secure web gateway in the Wireless Access Protection Section in the 3.1 Access Control Policy.
[b]	The Govern Team documents that corporate managed wireless access is not permitted in the Wireless Access Protection Section in the 3.1 Access Control Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.17[a]	Implemented

Assessment Objective

Wireless access to the system is protected using authentication

Program Procedure

The Govern Team documents that corporate managed wireless access is not permitted, and all wireless access must be protected by a virtual private network or secure web gateway in the Wireless Access Protection Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team Technical Lead

Process Summary

- The Technical Lead determines that corporate managed wireless access is not permitted.
- The Govern Team documents that corporate managed wireless access is not permitted in the Wireless Access Protection Section in the 3.1 Access Control Policy.

Process Evidence

Wireless Access Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.17[b]	Implemented

Assessment Objective

Wireless access to the system is protected using encryption

Program Procedure

The Govern Team documents that corporate managed wireless access is not permitted in the Wireless Access Protection Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team Technical Lead

Process Summary

- The Technical Lead determines that corporate managed wireless access is not permitted.
- The Govern Team documents that corporate managed wireless access is not permitted in the Wireless Access Protection Section in the 3.1 Access Control Policy.

Process Evidence

Wireless Access Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.18		Mobile Device Connection
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Control connection of mobile devices.

Procedure Summary

[a]	The Cybersecurity Program Director determines mobile devices that process, store, or transmit CUI are not allowed in the enclave and documents in the Mobile Device Connections Section in the 3.1 Access Control Policy.
[b]	The System Deployer configures the system such that no mobile device connections are allowed according to the System Baseline Standard.
[c]	The System Security Analyst monitors the SIEM for alerts that identify unauthorized mobile device usage.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.18[a]	Implemented

Assessment Objective

Mobile devices that process, store, or transmit CUI are identified

Program Procedure

The Cybersecurity Program Director determines mobile devices that process, store, or transmit CUI are not allowed in the enclave and documents in the Mobile Device Connections Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team System Designer

Process Summary

- The Cybersecurity Program Director decides that the organization does not have, and does not allow, mobile devices that process, store, or transmit CUI.
- The Govern Team documents that mobile devices are not allowed in the environment in the Mobile Device Connections Section in the 3.1 Access Control Policy.
- The System Designer develops the configuration to enforce the blocking of mobile connections.
- The System Designer documents the configuration to block mobile connections in the System Baseline Standard.

Process Evidence

Mobile Device Connections Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.18[b]	Implemented

Assessment Objective

Mobile device connections are authorized

Program Procedure

The System Deployer configures the system such that no mobile device connections are allowed according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-BlockRichClientOnAllMobile-EID in Microsoft Entra to block all mobile rich clients from connecting to the tenant.
- Configure Device Platform Restriction for all Android devices DPR-BlockAllAndroidMobileEnrollment-INT to block the enrollment of any mobile devices into MDM.
- Configure Device Platform Restriction for all Android devices DPR-BlockPersonalAndroidMobileEnrollment-INT to block the enrollment of personal devices into MDM.
- Configure Device Platform Restriction for all iOS devices DPR-BlockAlliOSMobileEnrollment-INT to block the enrollment of any mobile devices into MDM.
- Configure Device Platform Restriction for all iOS devices DPR-BlockPersonaliOSMobileEnrollment-INT to block the enrollment of personal devices into MDM.

Configuration Evidence

CAP-BlockRichClientOnAllMobile-EID
- Entra Admin Portal > Security > Conditional Access

DPR-BlockAllAndroidMobileDeviceEnrollment-INT
- Intune > Devices > Enrollment > Device Platform Restriction > Android Restrictions

DPR-BlockAlliOSMobileEnrollment-INT
- Intune > Devices > Enrollment > Device Platform Restriction > iOS Restrictions

DPR-BlockPersonalAndroidMobileEnrollment-INT
- Intune Portal > Devices > Enrollment > Device Platform Restrictions

DPR-BlockPersonaliOSMobileEnrollment-INT
- Intune Portal > Devices > Enrollment > Device Platform Restrictions

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.18[c]	Implemented

Assessment Objective
Mobile device connections are monitored and logged

Program Procedure
The System Security Analyst monitors the SIEM for alerts that identify unauthorized mobile device usage.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Create custom analytics rule SAR-MobileDeviceEnrollment-SEN to alert when new mobile devices are enrolled in the tenant.

Configuration Evidence

SAR-MobileDeviceEnrollment-SEN

- Azure Portal > Microsoft Sentinel > Analytics

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.19		Encrypt CUI On Mobile
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Encrypt CUI on mobile devices and mobile computing platforms.

Procedure Summary

[a]	The Govern Team documents that no physical mobile devices and mobile computing platforms containing CUI are permitted in the Encrypt CUI on Mobile Section in the 3.1 Access Control Policy.
[b]	The System Deployer configures systems such that no mobile devices or mobile computing platforms are permitted in the enclave according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.19[a]	Implemented

Assessment Objective

Mobile devices and mobile computing platforms that process, store, or transmit CUI are identified

Program Procedure

The Govern Team documents that no physical mobile devices and mobile computing platforms containing CUI are permitted in the Encrypt CUI on Mobile Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if physical mobile devices and mobile computing platforms are allowed in the environment.
- The Govern Team documents that no physical mobile devices and mobile computing platforms containing CUI are allowed in the environment in the Encrypt CUI on Mobile Section in the 3.1 Access Control Policy.

Process Evidence

Encrypt CUI on Mobile Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.19[b]	Implemented

Assessment Objective

Encryption is employed to protect CUI on identified mobile devices and mobile computing platforms

Program Procedure

The System Deployer configures systems such that no mobile devices or mobile computing platforms are permitted in the enclave according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-BlockRichClientOnAllMobile-EID in Microsoft Entra to block all mobile rich clients from connecting to the tenant.

Configuration Evidence

CAP-BlockRichClientOnAllMobile-EID

- Entra Admin Portal > Security > Conditional Access

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.20		External Connections
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Verify and control/limit connections to and use of external systems.

Procedure Summary

[a]	The Technical Lead identifies connections to external systems in the User, Process, and Asset Inventory.
[b]	The Technical Lead identifies the use of external systems in the User, Process, and Asset Inventory.
[c]	The System Security Analyst verifies connections to external systems in the Security Monitoring Output Log.
[d]	The System Security Analyst verifies the use of external systems in the Security Monitoring Output Log.
[e]	The System Deployer configures the system such that connections to external systems are controlled according to the System Baseline Standard.
[f]	The System Deployer configures the system such that the use of external systems is controlled according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.20[a]	Implemented

Assessment Objective

Connections to external systems are identified

Program Procedure

The Technical Lead identifies connections to external systems in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team Operate Team Technical Lead

Process Summary

- The Govern Team documents the policy for external system use and connections in the External Connections Section in the 3.1 Access Control Policy.
- The Technical Lead identifies external systems in the environment.
- The Operate Team documents external systems in the User, Process, and Asset Inventory.
- The Technical Lead identifies the method of connection to external systems in the environment.
- The Operate Team documents the methods of connection to external systems in the User, Process, and Asset Inventory.
- The Technical Lead identifies the use of the external system in the environment.
- The Operate Team documents the use of external systems in the User, Process, and Asset Inventory.
- The Technical Lead identifies the external system's accreditation.
- The Operate Team documents the external system's accreditation in the User, Process, and Asset Inventory.

Process Evidence

External Connections Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.20[b]	Implemented

Assessment Objective

The use of external systems is identified

Program Procedure

The Technical Lead identifies the use of external systems in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team Operate Team Technical Lead

Process Summary

- The Govern Team documents the policy for external system use and connections in the External Connections Section in the 3.1 Access Control Policy.
- The Technical Lead identifies external systems in the environment.
- The Operate Team documents external systems in the User, Process, and Asset Inventory.
- The Technical Lead identifies the method of connection to external systems in the environment.
- The Operate Team documents the methods of connection to external systems in the User, Process, and Asset Inventory.
- The Technical Lead identifies the use of the external system in the environment.
- The Operate Team documents the use of external systems in the User, Process, and Asset Inventory.
- The Technical Lead identifies the external system's accreditation.
- The Operate Team documents the external system's accreditation in the User, Process, and Asset Inventory.

Process Evidence

External Connections Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.20[c]	Implemented

Assessment Objective

Connections to external systems are verified

Program Procedure

The System Security Analyst verifies connections to external systems in the Security Monitoring Output Log.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- After connectors are set up, Defender XDR audits all cloud operations by default. Each audit log entry contains a user's immutable objectID that can be used to uniquely trace an individual system user to each action.
- Configure Conditional Access Policy CAP-BlockUntrustedLocations-EID to block connections from untrusted locations
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 AVD

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-BlockUntrustedLocations-EID

- Entra Admin Portal > Security > Conditional Access

CAP-EnforceRRMFA-EID

- Entra Admin Portal > Security > Conditional Access

Microsoft CMMC Additional Controls Learn Article

- https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-additional-controls

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.20[d]	Implemented

Assessment Objective

The use of external systems is verified

Program Procedure

The System Security Analyst verifies the use of external systems in the Security Monitoring Output Log.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Create Named Location LOC-UntrustedLocations-ENT as a blocklist for conditional access policies
- Microsoft Sentinel provides audit reduction and report generation by default

Win 10/11 AVD

- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceConditionalAccessAppControlOnBrowser-EID
- Entra Admin Portal > Security > Conditional Access

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

LOC-UntrustedLocations-ENT
- Azure > Entra ID Conditional Access Policies > Manage > Named Locations

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.20[e]	Implemented

Assessment Objective

Connections to external systems are controlled/limited

Program Procedure

The System Deployer configures the system such that connections to external systems are controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure CAP-BlockBrowserUnmanagedDeviceV1.1-EID to block browser access from unmanaged devices
- Configure Conditional Access Policy CAP-BlockUntrustedLocations-EID to block connections from untrusted locations
- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Microsoft Entra ID data connector to send audit, sign in and non-interactive sign in logs to the Log Analytics Workspace.

Win 10/11 AVD

- Configure CFG-BlockAVDClipboardRedirection-INT to block clipboard redirection to client endpoints from AVD sessions
- Configure CFG-BlockAVDDriveRedirection-INT to block drive redirection to client endpoints from AVD sessions.
- Configure CFG-BlockAVDPrinterRedirection-INT to block printer redirection to client endpoints from AVD sessions
- Configure CFG-BlockAVDUSBDriveRedirection-INT to block AVD drive redirection to client endpoints from AVD sessions
- Configure CFG-BlockClientScreenShotOnVirtualDesktopConnections-INT to disable screenshots of virtual machine sessions on client devices
- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure CFG-BlockClientScreenShotOnVirtualDesktopConnections-INT to disable screenshots of virtual machine sessions on client devices

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- Configure CFG-BlockW365ClipboardRedirection-INT to block clipboard redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365DriveRedirection-INT to block drive redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365PrinterRedirection-INT to block printer redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365USBDriveRedirection-INT to block USB drive redirection to client endpoints from W365 sessions
- Configure Conditional Access Policy CAP-EnforceConditionalAccessAppControlOnBrowser-EID to enforce routing of remote access through Microsoft Defender for Cloud Apps.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-BlockBrowserUnmanagedDeviceV1.1-EID
- Entra Admin Portal > Security > Conditional Access

CAP-BlockUntrustedLocations-EID
- Entra Admin Portal > Security > Conditional Access

CAP-EnforceConditionalAccessAppControlOnBrowser-EID
- Entra Admin Portal > Security > Conditional Access

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

CFG-BlockAVDClipboardRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDPrinterRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDUSBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockClientScreenShotOnVirtualDesktopConnections-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365ClipboardRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365DriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365PrinterRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365USBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Microsoft Entra ID Log Diagnostic Settings
- Entra ID > Monitoring > Diagnostic settings

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.20[f]	Implemented

Assessment Objective

The use of external systems is controlled/limited

Program Procedure

The System Deployer configures the system such that the use of external systems is controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure CAP-BlockBrowserUnmanagedDeviceV1.1-EID to block browser access from unmanaged devices
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Microsoft Entra ID data connector to send audit, sign in and non-interactive sign in logs to the Log Analytics Workspace.

Win 10/11 AVD

- Configure CFG-BlockAVDClipboardRedirection-INT to block clipboard redirection to client endpoints from AVD sessions
- Configure CFG-BlockAVDDriveRedirection-INT to block drive redirection to client endpoints from AVD sessions.
- Configure CFG-BlockAVDPrinterRedirection-INT to block printer redirection to client endpoints from AVD sessions
- Configure CFG-BlockAVDUSBDriveRedirection-INT to block AVD drive redirection to client endpoints from AVD sessions
- Configure CFG-BlockClientScreenShotOnVirtualDesktopConnections-INT to disable screenshots of virtual machine sessions on client devices
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure CFG-BlockClientScreenShotOnVirtualDesktopConnections-INT to disable screenshots of virtual machine sessions on client devices
- Configure CFG-BlockW365ClipboardRedirection-INT to block clipboard redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365DriveRedirection-INT to block drive redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365PrinterRedirection-INT to block printer redirection to client endpoints from W365 sessions

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- Configure CFG-BlockW365USBDriveRedirection-INT to block USB drive redirection to client endpoints from W365 sessions
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-BlockBrowserUnmanagedDeviceV1.1-EID
- Entra Admin Portal > Security > Conditional Access

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

CFG-BlockAVDClipboardRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDPrinterRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDUSBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockClientScreenShotOnVirtualDesktopConnections-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365ClipboardRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365DriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365PrinterRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365USBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Microsoft Entra ID Log Diagnostic Settings
- Entra ID > Monitoring > Diagnostic settings

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.21		Portable Storage Use
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Limit use of portable storage devices on external systems.

Procedure Summary

[a]	The Govern Team documents portable storage devices are not permitted in the Portable Storage Use Section in the 3.1 Access Control Policy.
[b]	The System Designer defines that the use of portable storage devices is blocked in the System Baseline Standard.
[c]	The System Deployer configures the system to block the use of portable storage devices following the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.21[a]	Implemented

Assessment Objective

The use of portable storage devices containing CUI on external systems is identified and documented

Program Procedure

The Govern Team documents portable storage devices are not permitted in the Portable Storage Use Section in the 3.1 Access Control Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines that portable storage devices are not permitted.
- The Govern Team documents that portable storage devices are not permitted in the Portable Storage Use Section in the 3.1 Access Control Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Portable Storage Use Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.21[b]	Implemented

Assessment Objective

Limits on the use of portable storage devices containing CUI on external systems are defined

Program Procedure

The System Designer defines that the use of portable storage devices is blocked in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	System Designer

Process Summary

- The System Designer develops the configurations to block the use of portable storage devices.
- The System Designer documents the configurations to block the use of portable storage devices in the System Baseline Standard.

Process Evidence

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.21[c]	Implemented

Assessment Objective

The use of portable storage devices containing CUI on external systems is limited as defined

Program Procedure

The System Deployer configures the system to block the use of portable storage devices following the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

Win 10/11 AVD

- Configure CFG-BlockAVDDriveRedirection-INT to block drive redirection to client endpoints from AVD sessions.
- Configure CFG-BlockAVDUSBDriveRedirection-INT to block AVD drive redirection to client endpoints from AVD sessions

Win 10/11 Win365

- Configure CFG-BlockW365DriveRedirection-INT to block drive redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365USBDriveRedirection-INT to block USB drive redirection to client endpoints from W365 sessions

Configuration Evidence

CFG-BlockAVDDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDUSBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365DriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365USBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AC.L2-3.1.22		Control Public Information
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Control CUI posted or processed on publicly accessible systems.

Procedure Summary

[a]	The Cybersecurity Program Director identifies the Authorized Publishers and Authorized Publication Reviewers in the User, Process, and Asset Inventory.
[b]	The Govern Team documents the publication review process in the Publication Review Procedure.
[c]	The Authorized Publisher reviews the post before publication and documents in the Publication Review Log with the date and time the review was completed.
[d]	The Authorized Publication Reviewer reviews the post after publication and documents in the Publication Review Log with the date and time the review was completed.
[e]	The Cybersecurity Program Director ensures processes to remove or address improper posting of CUI are in place.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.22[a]	Implemented

Assessment Objective

Individuals authorized to post or process information on publicly accessible systems are identified

Program Procedure

The Cybersecurity Program Director identifies the Authorized Publishers and Authorized Publication Reviewers in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team Operate Team

Process Summary

- The Govern Team documents the Controlling Public Information Section in the 3.1 Access Control Policy.
- The Cybersecurity Program Director identifies Authorized Publishers.
- The Cybersecurity Program Director identifies Authorized Publication Reviewers.
- The Operate Team documents Authorized Publishers in the User, Process, and Asset Inventory.
- The Operate Team documents Authorized Publication Reviewers in the User, Process, and Asset Inventory.

Process Evidence

Controlling Public Information Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.22[b]	Implemented

Assessment Objective

Procedures to ensure CUI is not posted or processed on publicly accessible systems are identified

Program Procedure

The Govern Team documents the publication review process in the Publication Review Procedure.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents the publication review process in the Publication Review Procedure.

Process Evidence

Publication Review Procedure
- SharePoint > Govern Docs > Artifacts > Publication Review Procedure

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.22[c]	Implemented

Assessment Objective

A review process is in place prior to posting of any content to publicly accessible systems

Program Procedure

The Authorized Publisher reviews the post before publication and documents in the Publication Review Log with the date and time the review was completed.

Procedure Type	Responsible Role	Supporting Roles
Process	Authorized Publisher	Authorized Publisher

Process Summary

- The Authorized Publisher reviews the post prior to publishing, and documents the Pre-Publication Review section of the Publication Review Log.
- The Authorized Publisher publishes the post to the publicly accessible system and documents the Published section of the Publication Review Log.

Process Evidence

Publication Review Log
- SharePoint > Govern Docs > Artifacts > Publication Review Log

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.22[d]	Implemented

Assessment Objective

Content on publicly accessible systems is reviewed to ensure that it does not include CUI

Program Procedure

The Authorized Publication Reviewer reviews the post after publication and documents in the Publication Review Log with the date and time the review was completed.

Procedure Type	Responsible Role	Supporting Roles
Process	Authorized Publication Reviewer	Authorized Publication Reviewer Authorized Publisher

Process Summary

- The Authorized Publication Reviewer reviews the post after publication and documents the Post-Publication Review section of the Publication Review Log.
- The Authorized Publisher publishes the post to the publicly accessible system and documents the Published section of the Publication Review Log.

Process Evidence

Publication Review Log
- SharePoint > Govern Docs > Artifacts > Publication Review Log

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.1.22[e]	Implemented

Assessment Objective

Mechanisms are in place to remove and address improper posting of CUI

Program Procedure

The Cybersecurity Program Director ensures processes to remove or address improper posting of CUI are in place.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Authorized Publisher Cybersecurity Program Director Technical Lead

Process Summary

- The Cybersecurity Program Director identifies authorized publicly accessible systems in the User, Process, and Asset Inventory.
- The Technical Lead documents the publication removal mechanism SOP in the User, Process, and Asset Inventory.
- The Authorized Publisher submits Event Investigation Case via the support portal for suspected sensitive data spillage.
- The Cybersecurity Program Director convenes the Incident Response Team (IRT) to determine if event is determined to be an incident.
- The Cybersecurity Program Director initiates the Incident Response Plan if event is determined to be an incident.
- The Authorized Publisher removes the post via the documented publication removal mechanism.
- The Authorized Publisher documents the date and time of the post was removed in the Removal section of the Publication Review Log.

Process Evidence

Event Investigation Case
- support.ardalyst.com

Incident Response Case
- support.ardalyst.com

Incident Response Plan
- SharePoint > Govern Docs > Artifacts > Incident Response Plan

Publication Review Log
- SharePoint > Govern Docs > Artifacts > Publication Review Log

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Practice Code		Practice Name
AT.L2-3.2.1		Role-Based Risk Awareness
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

Procedure Summary

[a]	The Govern Team performs the Risk Assessment according to 3.11 Risk Assessment Policy.
[b]	The Cybersecurity Program Director documents the Acceptable Use Policy.
[c]	The Authorized User signs Acceptable Use Policy, indicating their awareness of security risks associated with their activities.
[d]	The Privileged User signs the Privileged User Acceptable Use Policy, indicating their awareness of security risks associated with their activities.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.2.1[a]	Implemented

Assessment Objective

Security risks associated with organizational activities involving CUI are identified

Program Procedure

The Govern Team performs the Risk Assessment according to 3.11 Risk Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents the Role-Based Risk Awareness Section in the 3.2 Awareness and Training Policy.
- The Govern Team conducts a risk assessment based on the completed Scope Enclave Diagram and CUI Flow Diagram.

Process Evidence

Risk Assessment
- SharePoint > Govern Docs > Artifacts > Risk Assessment

Role-Based Risk Awareness Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.2 Awareness and Training Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.2.1[b]	Implemented

Assessment Objective

Policies, standards, and procedures related to the security of the system are identified

Program Procedure

The Cybersecurity Program Director documents the Acceptable Use Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team

Process Summary

- The Govern Team documents the Role-Based Risk Awareness Section in the 3.2 Awareness and Training Policy.
- The Cybersecurity Program Director documents the Acceptable Use Policy.
- The Govern Team documents the Privileged User Acceptable Use Policy.

Process Evidence

Acceptable Use Policy
- SharePoint > Govern Docs > Artifacts > Acceptable Use Policy

Privileged User Acceptable Use Policy
- SharePoint > Govern Docs > Artifacts > Privileged User Acceptable Use Policy

Role-Based Risk Awareness Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.2 Awareness and Training Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.2.1[c]	Implemented

Assessment Objective

Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities

Program Procedure

The Authorized User signs Acceptable Use Policy, indicating their awareness of security risks associated with their activities.

Procedure Type	Responsible Role	Supporting Roles
Process	Authorized User	Authorized User Govern Team Technical Lead

Process Summary

- The Govern Team documents the Role-Based Risk Awareness Section in the 3.2 Awareness and Training Policy.
- The Technical Lead defines training requirements in the User, Process, and Asset Inventory.
- The Authorized User completes training prior to accessing organization systems, and annually thereafter.
- The Technical Lead records training completion in the User, Process, and Asset Inventory or training tracking system.
- The Authorized User signs the Acceptable Use Policy.

Process Evidence

Acceptable Use Policy
- SharePoint > Govern Docs > Artifacts > Acceptable Use Policy

Role-Based Risk Awareness Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.2 Awareness and Training Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.2.1[d]	Implemented

Assessment Objective

Managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system

Program Procedure

The Privileged User signs the Privileged User Acceptable Use Policy, indicating their awareness of security risks associated with their activities.

Procedure Type	Responsible Role	Supporting Roles
Process	Privileged User	Govern Team Privileged User

Process Summary

- The Govern Team documents the Role-Based Risk Awareness Section in the 3.2 Awareness and Training Policy.
- The Privileged User signs the Privileged User Acceptable Use Policy.

Process Evidence

Privileged User Acceptable Use Policy
- SharePoint > Govern Docs > Artifacts > Privileged User Acceptable Use Policy

Role-Based Risk Awareness Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.2 Awareness and Training Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AT.L2-3.2.2		Role-Based Training
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Procedure Summary

[a]	The Govern Team documents information security-related roles, duties, and responsibilities in the System Security Plan.
[b]	The Govern Team ensures information security related duties, roles, and responsibilities are assigned to all personnel in the User, Process, and Asset Inventory.
[c]	The Authorized User completes DoW CUI and Cybersecurity Awareness Training.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.2.2[a]	Implemented

Assessment Objective

Information security-related duties, roles, and responsibilities are defined

Program Procedure

The Govern Team documents information security-related roles, duties, and responsibilities in the System Security Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents training requirements in the Role-Based Risk Awareness Section in the 3.2 Awareness and Training Policy.
- The Govern Team documents the roles and responsibilities in the System Security Plan.

Process Evidence

Role-Based Risk Awareness Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.2 Awareness and Training Policy

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.2.2[b]	Implemented

Assessment Objective

Information security-related duties, roles, and responsibilities are assigned to designated personnel

Program Procedure

The Govern Team ensures information security related duties, roles, and responsibilities are assigned to all personnel in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Govern Team documents training requirements in the Role-Based Risk Awareness Section in the 3.2 Awareness and Training Policy.
- The Govern Team assigns roles to authorized External Service Provider personnel.
- The Cybersecurity Program Director assigns roles to authorized personnel based on the System Security Plan.
- The Govern Team documents assigned roles in the User, Process, and Asset Inventory.

Process Evidence

Role-Based Risk Awareness Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.2 Awareness and Training Policy

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.2.2[c]	Implemented

Assessment Objective

Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities

Program Procedure

The Authorized User completes DoW CUI and Cybersecurity Awareness Training.

Procedure Type	Responsible Role	Supporting Roles
Process	Authorized User	Authorized User Govern Team Human Resources Team Technical Lead

Process Summary

- The Govern Team documents training requirements in the Role-Based Risk Awareness Section in the 3.2 Awareness and Training Policy.
- The Human Resources Team stores user's training certificates.
- The Technical Lead defines training requirements in the User, Process, and Asset Inventory.
- The Authorized User completes training prior to accessing organization systems, and annually thereafter.
- The Technical Lead records training completion in the User, Process, and Asset Inventory or training tracking system.
- The Authorized User completes DoW CUI and Cybersecurity Awareness Training.

Process Evidence

Completed Training Certificate
- SharePoint > Govern Docs > Artifacts > Completed Training Certificate Folder

Role-Based Risk Awareness Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.2 Awareness and Training Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AT.L2-3.2.3		Insider Threat Awareness
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Procedure Summary

[a]	The Govern Team defines insider threat indicators according to DoW standards for Insider Threat Awareness.
[b]	The Authorized User completes DoW insider threat awareness training.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.2.3[a]	Implemented

Assessment Objective

Potential indicators associated with insider threats are identified

Program Procedure

The Govern Team defines insider threat indicators according to DoW standards for Insider Threat Awareness.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents insider threat indicators in the Insider Threat Awareness Section in the 3.2 Awareness and Training Policy.
- The Govern Team documents insider threat awareness training requirements in the Insider Threat Awareness Section of the 3.2 Awareness and Training Policy.

Process Evidence

Insider Threat Awareness Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.2 Awareness and Training Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.2.3[b]	Implemented

Assessment Objective

Security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees

Program Procedure

The Authorized User completes DoW insider threat awareness training.

Procedure Type	Responsible Role	Supporting Roles
Process	Authorized User	Authorized User Govern Team Human Resources Team Technical Lead

Process Summary

- The Govern Team documents insider threat awareness training requirements in the Insider Threat Awareness Section of the 3.2 Awareness and Training Policy.
- The Technical Lead defines training requirements in the User, Process, and Asset Inventory.
- The Authorized User completes insider threat awareness training.
- The Technical Lead records training completion in the User, Process, and Asset Inventory or training tracking system.
- The Human Resources Team or designee stores user's completed training certificates in the Completed Training Certificate.

Process Evidence

Completed Training Certificate
- SharePoint > Govern Docs > Artifacts > Completed Training Certificate Folder

Insider Threat Awareness Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.2 Awareness and Training Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AU.L2-3.3.1		System Auditing
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

Procedure Summary

[a]	The System Designer specifies the configuration for audit logs in the System Catalog.
[b]	The System Designer defines the configuration for audit log contents in the System Catalog.
[c]	The System Security Analyst configures systems such that they meet audit log requirements according to the System Baseline Standard.
[d]	The System Security Analyst configures systems such that they meet audit log content requirements according to the System Baseline Standard.
[e]	The Technical Lead determines the organization's audit retention requirements as no less than ninety (90) days in the System Auditing Section in the 3.3 Audit and Accountability Policy.
[f]	The System Security Analyst configures systems such that they are retained for no less than ninety (90) days according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.1[a]	Implemented

Assessment Objective

Audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified

Program Procedure

The System Designer specifies the configuration for audit logs in the System Catalog.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for audit logs in the System Auditing Section in the 3.3 Audit and Accountability Policy.
- The System Designer develops the configurations for audit log types.
- The System Designer documents the configurations for audit log types in the System Catalog.

Process Evidence

System Auditing Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.1[b]	Implemented

Assessment Objective

The content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined

Program Procedure

The System Designer defines the configuration for audit log contents in the System Catalog.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for audit log contents in the System Auditing Section in the 3.3 Audit and Accountability Policy.
- The System Designer develops the configurations for audit log contents.
- The System Designer documents the configurations for audit log types in the System Catalog.

Process Evidence

System Auditing Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.1[c]	Implemented

Assessment Objective

Audit records are created (generated)

Program Procedure

The System Security Analyst configures systems such that they meet audit log requirements according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- After connectors are set up, Defender XDR audits all cloud operations by default. Each audit log entry contains a user's immutable objectID that can be used to uniquely trace an individual system user to each action.
- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Configure Log Analytics Workspace Data Retention to ninety (90) days.
- Configure User and Entity Behavior Analytics (UEBA) in Sentinel to enable further account auditing
- Enable Purview Unified Logs in Microsoft 365 to facilitate enhanced auditing
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default

Win 10/11 AVD

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Win 10/11 Win365

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Configuration Evidence

EDR-DeployDefenderConnector-INT
- Intune Portal > Endpoint Security > Endpoint Detection and Response

Log Analytics Workspace Data Retention
- Azure > Log Analytics Workspace > Settings > Usage and Estimated Costs > Data Retention

Microsoft CMMC Additional Controls Learn Article
- https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-additional-controls

Microsoft Defender XDR to Sentinel Connector Learn Article
- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

Purview Unified Logs
- purview.microsoft.us > Audit (under Solutions)

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Sentinel UEBA Settings Screenshot

- portal.azure.us > Microsoft Sentinel > [Workspace Name] > Entity Behavior > Entity Behavior Settings

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.1[d]	Implemented

Assessment Objective

Audit records, once created, contain the defined content

Program Procedure

The System Security Analyst configures systems such that they meet audit log content requirements according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- After connectors are set up, Defender XDR audits all cloud operations by default. Each audit log entry contains a user's immutable objectID that can be used to uniquely trace an individual system user to each action.
- Configure Log Analytics Workspace Data Retention to ninety (90) days.
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default

Win 10/11 AVD

- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Win 10/11 Win365

- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Configuration Evidence

Log Analytics Workspace Data Retention

- Azure > Log Analytics Workspace > Settings > Usage and Estimated Costs > Data Retention

Microsoft CMMC Additional Controls Learn Article

- https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-additional-controls

Microsoft Defender XDR to Sentinel Connector Learn Article

- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.1[e]	Implemented

Assessment Objective

Retention requirements for audit records are defined

Program Procedure

The Technical Lead determines the organization's audit retention requirements as no less than ninety (90) days in the System Auditing Section in the 3.3 Audit and Accountability Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Cybersecurity Program Director Govern Team System Designer Technical Lead

Process Summary

- The Cybersecurity Program Director defines retention requirements as no less than ninety (90) days.
- The Technical Lead specifies the organization's audit retention requirements as no less than ninety (90) days.
- The Govern Team documents the retention requirement for audit logs as no less than ninety (90) days in the System Auditing Section in the 3.3 Audit and Accountability Policy.
- The System Designer develops the configurations for the retention requirement for audit logs to be no less than ninety (90) days.
- The System Designer documents the configurations for the retention requirement for audit logs to be no less than ninety (90) days in the System Baseline Standard.

Process Evidence

Audit Retention Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

System Auditing Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.1[f]	Implemented

Assessment Objective

Audit records are retained as defined

Program Procedure

The System Security Analyst configures systems such that they are retained for no less than ninety (90) days according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Configure Log Analytics Workspace Data Retention to ninety (90) days.

Configuration Evidence

Log Analytics Workspace Data Retention

- Azure > Log Analytics Workspace > Settings > Usage and Estimated Costs > Data Retention

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AU.L2-3.3.2		User Accountability
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Procedure Summary

[a]	The System Designer develops user tracing in audit records in the System Baseline Standard.
[b]	The System Deployer configures systems such that audit records are traced to users according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.2[a]	Implemented

Assessment Objective

The content of the audit records needed to support the ability to uniquely trace users to their actions is defined

Program Procedure

The System Designer develops user tracing in audit records in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents that systems must trace actions to unique users in audit records in the User Accountability Section in the 3.3 Audit and Accountability Policy.
- The System Designer develops the configuration to ensure audit records are traced to users.
- The System Designer documents definitions for the content of the audit records in the System Catalog.
- The System Designer documents the configuration to ensure audit records are traced to users in the System Baseline Standard.

Process Evidence

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

User Accountability Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.2[b]	Implemented

Assessment Objective

Audit records, once created, contain the defined content

Program Procedure

The System Deployer configures systems such that audit records are traced to users according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- After connectors are set up, Defender XDR audits all cloud operations by default. Each audit log entry contains a user's immutable objectID that can be used to uniquely trace an individual system user to each action.
- Enable Purview Unified Logs in Microsoft 365 to facilitate enhanced auditing
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Win 10/11 AVD

- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Win 10/11 Win365

- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Configuration Evidence

Microsoft CMMC Additional Controls Learn Article
- https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-additional-controls

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Purview Unified Logs
- purview.microsoft.us > Audit (under Solutions)

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AU.L2-3.3.3		Event Review
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Review and update logged events.

Procedure Summary

[a]	The System Security Analyst determines when to review logged events according to Event Review Section in the 3.3 Audit and Accountability Policy.
[b]	The System Security Analyst conducts the event review process according to Event Review Section in the 3.3 Audit and Accountability Policy.
[c]	The System Security Analyst updates the event types being logged based on the review according to Event Review Section in the 3.3 Audit and Accountability Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.3[a]	Implemented

Assessment Objective
A process for determining when to review logged events is defined

Program Procedure
The System Security Analyst determines when to review logged events according to Event Review Section in the 3.3 Audit and Accountability Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	System Security Analyst	Defend Team Govern Team

Process Summary

- The Defend Team defines the process and timing for the review of logged events.
- The Govern Team documents the process for event review in the Event Review Section in the 3.3 Audit and Accountability Policy.

Process Evidence

Event Review Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.3[b]	Implemented

Assessment Objective

Event types being logged are reviewed in accordance with the defined review process

Program Procedure

The System Security Analyst conducts the event review process according to Event Review Section in the 3.3 Audit and Accountability Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	System Security Analyst	System Security Analyst

Process Summary

- The System Security Analyst initiates the event review process.
- The System Security Analyst interviews Defend Team members to understand what alerts need to be reviewed.
- The System Security Analyst reviews alerts flagged as false positive.
- The System Security Analyst identifies a new alert to add to event monitoring, opens a Change Control Request Case, and assigns to the System Maintainer.
- The System Security Analyst opens a Change Control Request Case to change alert logic.
- The System Security Analyst documents out the Name, Date, and Alert Tuning Details in the Alert Tuning Log.

Process Evidence

Alert Tuning Log
- SharePoint > Govern Docs > Artifacts > Alert Tuning Log

Change Control Request Case
- support.ardalyst.com

Event Review Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

Security Monitoring Output Log
- SharePoint > Govern Docs > Artifacts > Security Monitoring Output Log

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Assessment Objective Identifier	Assessment Objective Status
3.3.3[c]	Implemented

Assessment Objective

Event types being logged are updated based on the review

Program Procedure

The System Security Analyst updates the event types being logged based on the review according to Event Review Section in the 3.3 Audit and Accountability Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	System Security Analyst	System Security Analyst

Process Summary

- The System Security Analyst configures the new alert in the SIEM, and updates and closes the Change Control Request Case.
- The System Security Analyst changes the alert configurations, logs the change in the Change Control Request Case and closes the case.

Process Evidence

Change Control Request Case
- support.ardalyst.com

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AU.L2-3.3.4		Audit Failure Alerting
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Alert in the event of an audit logging process failure.

Procedure Summary

[a]	The Govern Team identifies personnel to be alerted of auditing failure in the User, Process, and Asset Inventory.
[b]	The System Designer defines the types of audit failures that generate alerts in the System Baseline Standard.
[c]	The System Deployer configures the system such that identified personnel are alerted of audit failure according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.4[a]	Implemented

Assessment Objective

Personnel or roles to be alerted in the event of an audit logging process failure are identified

Program Procedure

The Govern Team identifies personnel to be alerted of auditing failure in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team Technical Lead

Process Summary

- The Govern Team identifies the requirements for audit failure alerting in the Audit Failure Alerting Section in the 3.3 Audit and Accountability Policy.
- The Technical Lead identifies the personnel to be alerted of auditing failure in the User, Process, and Asset Inventory by assigning the Defend role to them.
- The Govern Team documents the personnel to be alerted of auditing failure in the User, Process, and Asset Inventory by assigning the Defend role to them.

Process Evidence

Audit Failure Alerting Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.4[b]	Implemented

Assessment Objective

Types of audit logging process failures for which alert will be generated are defined

Program Procedure

The System Designer defines the types of audit failures that generate alerts in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for audit failure alerting in the Audit Failure Alerting Section in the 3.3 Audit and Accountability Policy.
- The System Designer defines the types of audit failures that generate alerts.
- The System Designer documents the types of audit failures that generate alerts in the System Baseline Standard.

Process Evidence

Audit Failure Alerting Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.4[c]	Implemented

Assessment Objective

Identified personnel or roles are alerted in the event of an audit logging process failure

Program Procedure

The System Deployer configures the system such that identified personnel are alerted of audit failure according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Service Health Alert SHA-AuditFailureAlerting-AZR to alert the distribution group auditfailurealerting@ardalyst.com for audit failure alerts.
- Configure Service Health Alerts in the M365 admin center to alert the distribution group auditfailurealerting@ardalyst.com for audit failure alerts.

Configuration Evidence

M365 Service Health Alerts

- Microsoft Admin Center (portal.office365.us/adminportal) > Show all > Health > Service Health > Customize > Email

SHA-AuditFailureAlerting-AZR

- Azure > Service Health > Alerts > Health Alerts

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AU.L2-3.3.5		Audit Correlation
SPRS Value	**SPRS Score**	**Practice Status**
5	5	Implemented

Practice Statement

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

Procedure Summary

[a]	The System Designer documents the configuration for audit correlation in the System Baseline Standard.
[b]	The System Deployer configures systems such that they correlate audit records according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.5[a]	Implemented

Assessment Objective

Audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined

Program Procedure

The System Designer documents the configuration for audit correlation in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for audit correlation in the Audit Correlation Section in the 3.3 Audit and Accountability Policy.
- The System Designer develops the configuration for audit correlation.
- The System Designer documents the configuration for audit correlation in the System Baseline Standard.

Process Evidence

Audit Correlation Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.5[b]	Implemented

Assessment Objective

Defined audit record review, analysis, and reporting processes are correlated

Program Procedure

The System Deployer configures systems such that they correlate audit records according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Microsoft Defender XDR Connector to forward XDR event logs to Sentinel
- Create Diagnostic Settings for Azure Bastions to centralize Bastion logs in Sentinel
- Create Diagnostic Settings for Azure Firewalls to centralize Firewall logs in Sentinel
- Create Diagnostic Settings for Azure Network Security Groups to centralize Network Security Group logs in Sentinel
- Create Entra ID Diagnostic Setting to centralize Entra logs in Sentinel
- Create Intune Diagnostic Setting to forward Intune logs to Sentinel
- Deploy Azure Activity Connector in Microsoft Sentinel to Facilitate Enhanced Auditing
- Deploy Microsoft Defender for Cloud Connector in Microsoft Sentinel to Facilitate Centralized Security Monitoring
- Deploy the Microsoft 365 Sentinel Connector to centralize Office activity logs in Sentinel.
- Deploy the Microsoft Defender for Cloud Apps Sentinel Connector to centralize cloud app discovery and alert logs in Sentinel.
- Deploy the Microsoft Defender for Endpoint Sentinel Connector to centralize endpoint activity and alert logs in Sentinel.
- Deploy the Microsoft Defender for Identity Sentinel Connector to centralize identity activity and alert logs in Sentinel.
- Deploy the Microsoft Defender XDR Sentinel Connector to centralize unified security incidents, alerts, and entities in Sentinel.
- Deploy the Microsoft Entra ID Protection Sentinel Connector to centralize identity risk detections and automated threat alerts in Sentinel.
- Deploy the Microsoft Entra ID Sentinel Connector to centralize identity authentication and directory audit logs in Sentinel.
- Deploy the Windows Firewall Sentinel Connector to centralize Windows firewall logs in Sentinel
- Enable "Auditing and health monitoring" in Sentinel to enable monitoring of Sentinel workspace

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- Microsoft Sentinel uses pre-built detections to correlate audit logs and raise alerts by default

Configuration Evidence

Azure Activity Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Azure Bastions Diagnostic Settings
- portal.azure.us >Bastions > [bastion name] > Monitoring > Diagnostic settings

Azure Firewalls Diagnostic Settings
- portal.azure.us > Firewalls > [firewall name] > Monitoring > Diagnostic settings

Azure Network Security Groups Diagnostic Settings
- portal.azure.us > Network Security Groups > [network security group name] > Monitoring > Diagnostic settings

Defender XDR Connector Tables
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors > Microsoft Defender XDR

Intune Diagnostic Setting
- intune.microsoft.us > Reports > Azure monitor > Diagnostic settings

Microsoft 365 Sentinel Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Microsoft Defender for Cloud Apps
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Microsoft Defender for Cloud Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Microsoft Defender for Endpoint Sentinel Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Microsoft Defender for Identity Sentinel Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Microsoft Defender XDR Sentinel Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Microsoft Entra ID Log Diagnostic Settings
- Entra ID > Monitoring > Diagnostic settings

Microsoft Entra ID Protection Sentinel Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Microsoft Entra ID Sentinel Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Sentinel Health Monitoring
- portal.azure.us > Microsoft Sentinel > [workspace name] > Configuration > Settings > "Settings" tab > Auditing and health monitoring

Windows Firewall Sentinel Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AU.L2-3.3.6		Reduction and Reporting
SPRS Value	**SPRS Score**	**Practice Status**
1	1	Implemented

Practice Statement

Provide audit record reduction and report generation to support on-demand analysis and reporting.

Procedure Summary

[a]	The System Deployer configures the SIEM such that it provides audit reduction and on-demand analysis according to the System Baseline Standard.
[b]	The System Deployer configures the SIEM such that it provides audit report generation on-demand according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.6[a]	Implemented

Assessment Objective

An audit record reduction capability that supports on-demand analysis is provided

Program Procedure

The System Deployer configures the SIEM such that it provides audit reduction and on-demand analysis according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Deploy the Microsoft Defender XDR Sentinel Connector to centralize unified security incidents, alerts, and entities in Sentinel.
- Deploy the Microsoft Entra ID Protection Sentinel Connector to centralize identity risk detections and automated threat alerts in Sentinel.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default
- Microsoft Sentinel provides audit reduction and report generation by default

Configuration Evidence

Microsoft Defender XDR Sentinel Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Microsoft Defender XDR to Sentinel Connector Learn Article
- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

Microsoft Entra ID Protection Sentinel Connector
- portal.azure.us > Microsoft Sentinel > Configuration > Data Connectors

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.6[b]	Implemented

Assessment Objective

A report generation capability that supports on-demand reporting is provided

Program Procedure

The System Deployer configures the SIEM such that it provides audit report generation on-demand according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default
- Microsoft Sentinel provides audit reduction and report generation by default

Configuration Evidence

Microsoft Defender XDR to Sentinel Connector Learn Article
- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AU.L2-3.3.7		Authoritative Time Source
SPRS Value	**SPRS Score**	**Practice Status**
1	1	Implemented

Practice Statement

Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

Procedure Summary

[a]	The System Deployer configures the system such that internal system clocks use internal time stamps for audit records according to the System Baseline Standard.
[b]	The System Designer documents the authoritative time source in the System Baseline Standard.
[c]	The System Deployer configures the system such that internal clocks synchronize with the authoritative time source according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.7[a]	Implemented

Assessment Objective

Internal system clocks are used to generate time stamps for audit records

Program Procedure

The System Deployer configures the system such that internal system clocks use internal time stamps for audit records according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.
- Microsoft maintains its own authoritative time source for its datacenters by default.

Win 10/11 AVD

- Configure CFG-AuthoritativeTimeSource-INT to set windows endpoints to time.windows.com
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Win 10/11 Win365

- Configure CFG-AuthoritativeTimeSource-INT to set windows endpoints to time.windows.com
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Configuration Evidence

CFG-AuthoritativeTimeSource-INT

- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.7[b]	Implemented

Assessment Objective

An authoritative source with which to compare and synchronize internal system clocks is specified

Program Procedure

The System Designer documents the authoritative time source in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for authoritative time sources in the Authoritative Time Source Section in the 3.3 Audit and Accountability Policy.
- The System Designer develops the configuration for authoritative time sources.
- The System Designer documents the configuration for authoritative time sources in the System Baseline Standard.

Process Evidence

Authoritative Time Source Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.7[c]	Implemented

Assessment Objective

Internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source

Program Procedure

The System Deployer configures the system such that internal clocks synchronize with the authoritative time source according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft maintains its own authoritative time source for its datacenters by default.

Win 10/11 AVD

- Configure CFG-AuthoritativeTimeSource-INT to set windows endpoints to time.windows.com

Win 10/11 Win365

- Configure CFG-AuthoritativeTimeSource-INT to set windows endpoints to time.windows.com

Configuration Evidence

CFG-AuthoritativeTimeSource-INT

- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AU.L2-3.3.8		Audit Protection
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Procedure Summary

[a]	The System Deployer configures the system such that audit information is protected from unauthorized access according to the System Baseline Standard.
[b]	The System Deployer configures the system such that audit information is protected from unauthorized modification according to the System Baseline Standard.
[c]	The System Deployer configures the system such that audit information is protected from unauthorized deletion according to the System Baseline Standard.
[d]	The System Deployer configures the system such that audit logging tools are protected from unauthorized access according to the System Baseline Standard.
[e]	The System Deployer configures the system such that audit logging tools are protected from unauthorized modification according to the System Baseline Standard.
[f]	The System Deployer configures the system such that audit logging tools are protected from unauthorized deletion according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.8[a]	Implemented

Assessment Objective

Audit information is protected from unauthorized access

Program Procedure

The System Deployer configures the system such that audit information is protected from unauthorized access according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Log Analytics Workspace Data Retention to ninety (90) days.
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 AVD

- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 Win365

- Only subscription owners or contributors may change log retention duration by default.

Configuration Evidence

Log Analytics Workspace Data Retention

- Azure > Log Analytics Workspace > Settings > Usage and Estimated Costs > Data Retention

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.8[b]	Implemented

Assessment Objective

Audit information is protected from unauthorized modification

Program Procedure

The System Deployer configures the system such that audit information is protected from unauthorized modification according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Log Analytics Workspace Data Retention to ninety (90) days.
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 AVD

- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 Win365

- Only subscription owners or contributors may change log retention duration by default.

Configuration Evidence

Log Analytics Workspace Data Retention

- Azure > Log Analytics Workspace > Settings > Usage and Estimated Costs > Data Retention

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.8[c]	Implemented

Assessment Objective

Audit information is protected from unauthorized deletion

Program Procedure

The System Deployer configures the system such that audit information is protected from unauthorized deletion according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Log Analytics Workspace Data Retention to ninety (90) days.
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 AVD

- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 Win365

- Only subscription owners or contributors may change log retention duration by default.

Configuration Evidence

Log Analytics Workspace Data Retention

- Azure > Log Analytics Workspace > Settings > Usage and Estimated Costs > Data Retention

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.8[d]	Implemented

Assessment Objective

Audit logging tools are protected from unauthorized access

Program Procedure

The System Deployer configures the system such that audit logging tools are protected from unauthorized access according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Log Analytics Workspace Data Retention to ninety (90) days.
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 AVD

- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 Win365

- Only subscription owners or contributors may change log retention duration by default.

Configuration Evidence

Log Analytics Workspace Data Retention

- Azure > Log Analytics Workspace > Settings > Usage and Estimated Costs > Data Retention

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.8[e]	Implemented

Assessment Objective

Audit logging tools are protected from unauthorized modification

Program Procedure

The System Deployer configures the system such that audit logging tools are protected from unauthorized modification according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Log Analytics Workspace Data Retention to ninety (90) days.
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 AVD

- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 Win365

- Only subscription owners or contributors may change log retention duration by default.

Configuration Evidence

Log Analytics Workspace Data Retention

- Azure > Log Analytics Workspace > Settings > Usage and Estimated Costs > Data Retention

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.8[f]	Implemented

Assessment Objective

Audit logging tools are protected from unauthorized deletion

Program Procedure

The System Deployer configures the system such that audit logging tools are protected from unauthorized deletion according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Log Analytics Workspace Data Retention to ninety (90) days.
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 AVD

- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 Win365

- Only subscription owners or contributors may change log retention duration by default.

Configuration Evidence

Log Analytics Workspace Data Retention

- Azure > Log Analytics Workspace > Settings > Usage and Estimated Costs > Data Retention

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
AU.L2-3.3.9		Audit Management
SPRS Value	**SPRS Score**	**Practice Status**
1	1	Implemented

Practice Statement

Limit management of audit logging functionality to a subset of privileged users.

Procedure Summary

[a]	The System Designer defines a subset of privileged users able to manage audit logging functionality.
[b]	The System Deployer configures systems such that access to audit logs is limited to a subset of privileged users according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.9[a]	Implemented

Assessment Objective

A subset of privileged users granted access to manage audit logging functionality is defined

Program Procedure

The System Designer defines a subset of privileged users able to manage audit logging functionality.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for audit management in the Audit Management Section in the 3.3 Audit and Accountability Policy.
- The System Designer develops the configuration for limiting audit access.
- The System Designer documents the configuration for limiting audit access in the System Baseline Standard.

Process Evidence

Audit Management Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.3 Audit and Accountability Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.3.9[b]	Implemented

Assessment Objective

Management of audit logging functionality is limited to the defined subset of privileged users

Program Procedure

The System Deployer configures systems such that access to audit logs is limited to a subset of privileged users according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 AVD

- Only subscription owners or contributors may change log retention duration by default.

Win 10/11 Win365

- Only subscription owners or contributors may change log retention duration by default.

Configuration Evidence

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CM.L2-3.4.1		System Baselining
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Procedure Summary

[a]	The System Designer establishes the System Baseline Standard.
[b]	The System Designer includes all hardware, software, firmware, and documentation in the System Catalog.
[c]	The System Designer maintains the System Baseline Standard.
[d]	The Operate Team establishes the User, Process, and Asset Inventory.
[e]	The Operate Team includes all hardware, software, firmware, and documentation in the User, Process, and Asset Inventory.
[f]	The Operate Team maintains the User, Process, and Asset Inventory.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.1[a]	Implemented

Assessment Objective

A baseline configuration is established

Program Procedure

The System Designer establishes the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for system baselining in the System Baselining Section in the 3.4 Configuration Management Policy.
- The Govern Team documents a template for the System Baseline Standard.
- The System Designer documents the system baselines in the System Baseline Standard.
- The System Designer documents the system properties in the System Catalog.

Process Evidence

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

System Baselining Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.1[b]	Implemented

Assessment Objective

The baseline configuration includes hardware, software, firmware, and documentation

Program Procedure

The System Designer includes all hardware, software, firmware, and documentation in the System Catalog.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	System Designer

Process Summary

- The System Designer includes all hardware, software, firmware, and documentation in the System Catalog.

Process Evidence

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.1[c]	Implemented

Assessment Objective

The baseline configuration is maintained (reviewed and updated) throughout the system development life cycle

Program Procedure

The System Designer maintains the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	System Designer

Process Summary

- The System Designer receives a Change Control Request Case.
- The System Designer updates the System Baseline Standard to reflect the changes in the case.

Process Evidence

Change Control Request Case
- support.ardalyst.com

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.1[d]	Implemented

Assessment Objective

A system inventory is established

Program Procedure

The Operate Team establishes the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Operate Team	Govern Team Operate Team

Process Summary

- The Govern Team documents a template for the System Baseline Standard.
- The Operate Team documents organization assets in the User, Process, and Asset Inventory.

Process Evidence

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.1[e]	Implemented

Assessment Objective
The system inventory includes hardware, software, firmware, and documentation

Program Procedure
The Operate Team includes all hardware, software, firmware, and documentation in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Operate Team	Operate Team

Process Summary

- The Operate Team includes all hardware, software, firmware, and documentation in the User, Process, and Asset Inventory.

Process Evidence

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.1[f]	Implemented

Assessment Objective

The inventory is maintained (reviewed and updated) throughout the system development life cycle

Program Procedure

The Operate Team maintains the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Operate Team	Operate Team

Process Summary

- The Operate Team receives an Identity and Access Management Case.
- The Operate Team updates the User, Process, and Asset Inventory to reflect the changes in the case.

Process Evidence

Identity and Access Management Case
- support.ardalyst.com

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CM.L2-3.4.2		Security Configuration Enforcement
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Establish and enforce security configuration settings for information technology products employed in organizational systems.

Procedure Summary

[a]	The System Designer documents the configurations for security settings in the System Baseline Standard.
[b]	The System Deployer configures the system such that security configuration settings are enforced across all systems according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.2[a]	Implemented

Assessment Objective

Security configuration settings for information technology products employed in the system are established and included in the baseline configuration

Program Procedure

The System Designer documents the configurations for security settings in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for security configuration settings in the Security Configuration Enforcement Section in the 3.4 Configuration Management Policy.
- The System Designer develops the configurations for security settings.
- The System Designer documents the configurations for security settings in the System Baseline Standard.

Process Evidence

Security Configuration Enforcement Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.2[b]	Implemented

Assessment Objective

Security configuration settings for information technology products employed in the system are enforced

Program Procedure

The System Deployer configures the system such that security configuration settings are enforced across all systems according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Create "GRP-NonPrivUsers-EID" dynamic group to use with conditional access policies
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 AVD

- Configure "CFG-RequireSMBSigning-INT" to enforce SMB packet signing and mitigate SMB relay attacks.
- Configure CFG-RedirectHostMachineTimetoAVDSession-INT to allow the host machine to pass its time settings to the AVD.
- Configure Conditional Access Policy CAP-RequireWorkstationComplianceRichClientAccess-EID to require that workstations accessing through a rich client meet the device compliance policies
- Configure Dynamic Device Security Group "GRP-AllAVDs-EID" to include only Azure Virtual Desktops and Azure Virtual Machines for device management
- Configure Host Pool RDP Properties to enable quality of life features
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Configure "CFG-RequireSMBSigning-INT" to enforce SMB packet signing and mitigate SMB relay attacks.
- Configure Conditional Access Policy CAP-RequireWorkstationComplianceRichClientAccess-EID to require that workstations accessing through a rich client meet the device compliance policies
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Configuration Evidence

"GRP-NonPrivUsers-EID" Group
- Azure Admin Console -> Entra ID -> Groups

CAP-RequireWorkstationComplianceRichClientAccess-EID
- Entra Admin Portal > Security > Conditional Access

CFG-RedirectHostMachineTimetoAVDSession-INT
- Go to Intune Admin Center → Devices → Configuration

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

CFG-RequireSMBSigning-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

GRP-AllAVDs-EID
- Azure Admin Console -> Entra ID -> Groups

Host Pool RDP Properties
- Azure → host pool → Open the host pool → Settings → RDP Properties

Technical Reference Details About Encryption Learn Article
- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CM.L2-3.4.3		System Change Management
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Track, review, approve or disapprove, and log changes to organizational systems.

Procedure Summary

[a]	The Govern Team tracks changes in the Change Control Request Case.
[b]	The Cybersecurity Program Director reviews the changes according to the Change Management Section in the 3.4 Configuration Management Policy.
[c]	The Cybersecurity Program Director approves/disapproves the changes in the Change Control Request Case.
[d]	The System Deployer logs the change implementation in the Change Control Request Case.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.3[a]	Implemented

Assessment Objective

Changes to the system are tracked

Program Procedure

The Govern Team tracks changes in the Change Control Request Case.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Change Management Board Member Cybersecurity Program Director Defend Team Govern Team System Deployer System Designer

Process Summary

- The Govern Team documents the Change Control Process.
- The Govern Team documents the requirements for the Change Management Process in the Change Management Section in the 3.4 Configuration Management Policy.
- The Change Control Request Board receives a Change Control Request Case.
- The Govern Team develops the change to the organization documentation.
- The Govern Team documents the proposed changes to the organization documentation in the Change Control Request Case.
- The Govern Team identifies the System Designer for the system in question.
- The System Designer designs the proposed solution.
- The System Designer documents the proposed solution to the change request in the Change Control Request Case.
- The Defend Team conducts an SIA on the proposed solution.
- The Cybersecurity Program Director reviews the proposed solution.
- The Cybersecurity Program Director approves/disapproves the proposed change in the Disposition section of the Change Control Request Form.
- The Govern Team updates the organization documentation.
- The System Designer develops the configuration for the change.
- The System Designer documents the configuration for the change in the System Baseline Standard.
- The System Deployer configures the system such that it matches the System Baseline Standard.
- The System Deployer documents the deployment of the change in the Change Control Request Case.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- The System Deployer closes the Change Control Request Case after deployment.

Process Evidence

Change Control Process
- SharePoint > Govern Documents > Artifacts > Change Control Process

Change Control Request Case
- support.ardalyst.com

Change Control Request Form
- SharePoint > Govern Docs > Artifacts > Change Control Request Form

Change Management Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Assessment Objective Identifier	Assessment Objective Status
3.4.3[b]	Implemented

Assessment Objective

Changes to the system are reviewed

Program Procedure

The Cybersecurity Program Director reviews the changes according to the Change Management Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Change Management Board Member Cybersecurity Program Director Defend Team Govern Team System Deployer System Designer

Process Summary

- The Govern Team documents the requirements for the Change Management Process in the Change Management Section in the 3.4 Configuration Management Policy.
- The Change Control Request Board receives a Change Control Request Case.
- The Govern Team develops the change to the organization documentation.
- The Govern Team documents the proposed changes to the organization documentation in the Change Control Request Case.
- The Govern Team identifies the System Designer for the system in question.
- The System Designer designs the proposed solution.
- The System Designer documents the proposed solution to the change request in the Change Control Request Case.
- The Defend Team conducts an SIA on the proposed solution.
- The Cybersecurity Program Director reviews the proposed solution.
- The Cybersecurity Program Director approves/disapproves the proposed change in the Disposition section of the Change Control Request Form.
- The Govern Team updates the organization documentation.
- The System Designer develops the configuration for the change.
- The System Designer documents the configuration for the change in the System Baseline Standard.
- The System Deployer configures the system such that it matches the System Baseline Standard.
- The System Deployer documents the deployment of the change in the Change Control Request Case.
- The System Deployer closes the Change Control Request Case after deployment.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Process Evidence

Change Control Request Case
- support.ardalyst.com

Change Control Request Form
- SharePoint > Govern Docs > Artifacts > Change Control Request Form

Change Management Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.3[c]	Implemented

Assessment Objective

Changes to the system are approved or disapproved

Program Procedure

The Cybersecurity Program Director approves/disapproves the changes in the Change Control Request Case.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Change Management Board Member Cybersecurity Program Director Defend Team Govern Team System Deployer System Designer

Process Summary

- The Govern Team documents the requirements for the Change Management Process in the Change Management Section in the 3.4 Configuration Management Policy.
- The Change Control Request Board receives a Change Control Request Case.
- The Govern Team develops the change to the organization documentation.
- The Govern Team documents the proposed changes to the organization documentation in the Change Control Request Case.
- The Govern Team identifies the System Designer for the system in question.
- The System Designer designs the proposed solution.
- The System Designer documents the proposed solution to the change request in the Change Control Request Case.
- The Defend Team conducts an SIA on the proposed solution.
- The Cybersecurity Program Director reviews the proposed solution.
- The Cybersecurity Program Director approves/disapproves the proposed change in the Disposition section of the Change Control Request Form.
- The Govern Team updates the organization documentation.
- The System Designer develops the configuration for the change.
- The System Designer documents the configuration for the change in the System Baseline Standard.
- The System Deployer configures the system such that it matches the System Baseline Standard.
- The System Deployer documents the deployment of the change in the Change Control Request Case.
- The System Deployer closes the Change Control Request Case after deployment.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Process Evidence

Change Control Request Case
- support.ardalyst.com

Change Control Request Form
- SharePoint > Govern Docs > Artifacts > Change Control Request Form

Change Management Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.3[d]	Implemented

Assessment Objective

Changes to the system are logged

Program Procedure

The System Deployer logs the change implementation in the Change Control Request Case.

Procedure Type	Responsible Role	Supporting Roles
Process	System Deployer	Change Management Board Member Cybersecurity Program Director Defend Team Govern Team System Deployer System Designer

Process Summary

- The Govern Team documents the requirements for the Change Management Process in the Change Management Section in the 3.4 Configuration Management Policy.
- The Change Control Request Board receives a Change Control Request Case.
- The Govern Team develops the change to the organization documentation.
- The Govern Team documents the proposed changes to the organization documentation in the Change Control Request Case.
- The Govern Team identifies the System Designer for the system in question.
- The System Designer designs the proposed solution.
- The System Designer documents the proposed solution to the change request in the Change Control Request Case.
- The Defend Team conducts an SIA on the proposed solution.
- The Cybersecurity Program Director reviews the proposed solution.
- The Cybersecurity Program Director approves/disapproves the proposed change in the Disposition section of the Change Control Request Form.
- The Govern Team updates the organization documentation.
- The System Designer develops the configuration for the change.
- The System Designer documents the configuration for the change in the System Baseline Standard.
- The System Deployer configures the system such that it matches the System Baseline Standard.
- The System Deployer documents the deployment of the change in the Change Control Request Case.
- The System Deployer closes the Change Control Request Case after deployment.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Process Evidence
Change Control Request Case • support.ardalyst.com Change Control Request Form • SharePoint > Govern Docs > Artifacts > Change Control Request Form Change Management Section • SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy System Baseline Standard • SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CM.L2-3.4.4		Security Impact Analysis
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Analyze the security impact of changes prior to implementation.

Procedure Summary

[a]	The System Security Analyst analyzes security impact of changes to the system prior to implementation according to the Security Impact Analysis Section in the 3.4 Configuration Management Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.4[a]	Implemented

Assessment Objective

The security impact of changes to the system is analyzed prior to implementation

Program Procedure

The System Security Analyst analyzes security impact of changes to the system prior to implementation according to the Security Impact Analysis Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	System Security Analyst	Govern Team System Security Analyst

Process Summary

- The Govern Team documents the requirements for security impact analysis in the Security Impact Analysis Section in the 3.4 Configuration Management Policy.
- The System Security Analyst receives a Change Control Request Case from the support portal.
- The System Security Analyst conducts a Security Impact Analysis on the submitted Change Control Request Form.

Process Evidence

Change Control Request Case
- support.ardalyst.com

Security Impact Analysis
- SharePoint > Govern Docs > Artifacts > Security Impact Analysis

Security Impact Analysis Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Practice Code		Practice Name
CM.L2-3.4.5		Access Restrictions For Change
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

Procedure Summary

[a]	The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.
[b]	The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.
[c]	The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.
[d]	The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.
[e]	The System Designer develops logical access restrictions associated with changes in the System Baseline Standard.
[f]	The System Designer documents logical access restrictions associated with changes in the System Baseline Standard.
[g]	The Technical Lead approves the System Security Plan.
[h]	The System Deployer configures the system such that changes are restricted via logical access according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.5[a]	Implemented

Assessment Objective

Physical access restrictions associated with changes to the system are defined

Program Procedure

The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines there are no physical systems containing CUI.
- The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.

Process Evidence

Access Restrictions for Change Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.5[b]	Implemented

Assessment Objective

Physical access restrictions associated with changes to the system are documented

Program Procedure

The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines there are no physical systems containing CUI.
- The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.

Process Evidence

Access Restrictions for Change Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.5[c]	Implemented

Assessment Objective

Physical access restrictions associated with changes to the system are approved

Program Procedure

The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines there are no physical systems containing CUI.
- The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.

Process Evidence

Access Restrictions for Change Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.5[d]	Implemented

Assessment Objective

Physical access restrictions associated with changes to the system are enforced

Program Procedure

The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines there are no physical systems containing CUI.
- The Govern Team documents that the organization contains no physical systems containing CUI in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.

Process Evidence

Access Restrictions for Change Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.5[e]	Implemented

Assessment Objective

Logical access restrictions associated with changes to the system are defined

Program Procedure

The System Designer develops logical access restrictions associated with changes in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for logical access restrictions associated with changes in the Access Restrictions for Change Section in the 3.4 Configuration Management Policy.
- The System Designer develops logical access restrictions associated with changes in the System Baseline Standard.

Process Evidence

Access Restrictions for Change Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.5[f]	Implemented

Assessment Objective

Logical access restrictions associated with changes to the system are documented

Program Procedure

The System Designer documents logical access restrictions associated with changes in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	System Designer

Process Summary

- The System Designer documents logical access restrictions associated with changes in the System Baseline Standard.

Process Evidence

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.5[g]	Implemented

Assessment Objective
Logical access restrictions associated with changes to the system are approved

Program Procedure
The Technical Lead approves the System Security Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Technical Lead

Process Summary

- The Technical Lead approves the System Security Plan.

Process Evidence

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.5[h]	Implemented

Assessment Objective

Logical access restrictions associated with changes to the system are enforced

Program Procedure

The System Deployer configures the system such that changes are restricted via logical access according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.

Win 10/11 AVD

- Admins assigned to the “Virtual Machine Administrator Login” Role may perform local admin tasks on the AVD by default
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Users assigned to the “Virtual Machine User Login” RBAC Role may sign and use the AVD, but may not use local admin permissions by default

Win 10/11 Win365

- Configure CFG-ReplaceLocalAdmin-INT in Microsoft Intune to remove local administrator rights from users, and replace with select admins from Entra.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

AVD RBAC Roles

- Azure > Resource Groups > [AVD Resource Group] > [Example AVD] > Access Control (IAM) > Role Assignments

CAP-EnforceRRMFA-EID

- Entra Admin Portal > Security > Conditional Access

CFG-ReplaceLocalAdmin-INT

- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CM.L2-3.4.6		Least Functionality
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

Procedure Summary

[a]	The System Designer documents essential system capabilities in the System Catalog.
[b]	The System Deployer configures systems such that they only provide essential capabilities according to the System Catalog.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.6[a]	Implemented

Assessment Objective

Essential system capabilities are defined based on the principle of least functionality

Program Procedure

The System Designer documents essential system capabilities in the System Catalog.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for least functionality in the Least Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents essential system capabilities in the System Catalog.

Process Evidence

Least Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.6[b]	Implemented

Assessment Objective

The system is configured to provide only the defined essential capabilities

Program Procedure

The System Deployer configures systems such that they only provide essential capabilities according to the System Catalog.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Attack Surface Reduction Policy ASR-BlockMalCodeExecution-INT to block the use of malicious code
- Configure Conditional Access Policy CAP-BlockLegacyAuthentication-EID to block legacy authentication methods
- Configure Sentinel Analytic rule SAR-AdminLicenseAlert-SEN event is triggered when admins are assigned licenses

Win 10/11 AVD

- Configure "CFG-DisableCachedCredentials-INT" to disable storage of hashed credentials on Windows devices.
- Configure "CFG-DisableGuestAccount-INT" to disable the built-in Guest account on Windows devices.
- Configure "SCR-DisableAutoPlayForDefaultUserProfileOnWindowsDevices-INT" to disable Autoplay in the Default User Profile template on Windows devices.
- Configure "SCR-DisableWindowsAutoPlayOnWindowsDevices-INT" to disable Windows Explorer Autoplay on Windows devices.
- Configure Attack Surface Reduction Policy ASR-BlockMalCodeExecution-INT to block the use of malicious code
- Configure CFG-BlockNonessentialFunctionality-INT to block nonessential functionality on Windows devices.
- Configure CFG-TamperProtection-INT to enable Microsoft recommended antivirus settings (including real-time scans) and disable the ability for attackers to change them.
- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.

Win 10/11 Win365

- Configure "CFG-DisableCachedCredentials-INT" to disable storage of hashed credentials on Windows devices.
- Configure "CFG-DisableGuestAccount-INT" to disable the built-in Guest account on Windows devices.
- Configure "SCR-DisableAutoPlayForDefaultUserProfileOnWindowsDevices-INT" to disable Autoplay in the Default User Profile template on Windows devices.
- Configure "SCR-DisableWindowsAutoPlayOnWindowsDevices-INT" to disable Windows Explorer Autoplay on Windows devices.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- Configure Attack Surface Reduction Policy ASR-BlockMalCodeExecution-INT to block the use of malicious code
- Configure CFG-BlockNonessentialFunctionality-INT to block nonessential functionality on Windows devices.
- Configure CFG-TamperProtection-INT to enable Microsoft recommended antivirus settings (including real-time scans) and disable the ability for attackers to change them.
- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.

Configuration Evidence

ASR-BlockMalCodeExecution-INT
- Azure Admin Portal > Intune > Endpoint Security > Manage > Attack Surface Reduction

CAP-BlockLegacyAuthentication-EID
- Entra Admin Portal > Security > Conditional Access

CFG-BlockNonessentialFunctionality-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-DisableCachedCredentials-INT
- Intune > Devices > Manage Devices > Configuration

CFG-DisableGuestAccount-INT
- Intune > Devices > Manage Devices > Configuration

CFG-TamperProtection-INT
- Intune > Devices > Manage Devices > Configuration

SAR-AdminLicenseAlert-SEN Screenshot
- Sentinel > Configuration > Analytics

SCR-DisableWindowsAutoPlayOnWindowsDevices-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

SRC-DisableAutoPlayForDefaultUserProfileOnWindowsDevices-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

WCF-WebContentFiltering-DEF
- security.microsoft.us > system > settings > endpoints > rules > web content filtering

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CM.L2-3.4.7		Nonessential Functionality
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

Procedure Summary

[a]	The Cybersecurity Program Director defines programs essential to the organization according to the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
[b]	The Cybersecurity Program Director defines the programs not essential to the organization for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
[c]	The System Deployer configures the system to restrict, disable, or prevent the use of nonessential programs according to the System Baseline Standard.
[d]	The Cybersecurity Program Director defines the functions essential to the organization for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
[e]	The Cybersecurity Program Director defines the functions not essential to the organization for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
[f]	The System Deployer configures the system to restrict, disable, or prevent the use of nonessential functions according to the System Baseline Standard.
[g]	The Technical Lead defines the ports essential to the organization's IT operations for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
[h]	The Technical Lead defines the ports not essential to the organization's IT operations for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
[i]	The System Deployer configures the system to restrict, disable, or prevent the use of nonessential ports according to the System Baseline Standard.
[j]	The Technical Lead defines the protocols essential to the organization's IT operations for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
[k]	The Technical Lead defines the protocols not essential to the organization's IT operations for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
[l]	The System Deployer configures the system to restrict, disable, or prevent the use of nonessential protocols according to the System Baseline Standard.
[m]	The Technical Lead defines the services essential to the organization for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

[n]	The Technical Lead defines the services not essential to the organization's IT operations for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
[o]	The System Deployer configures the system to restrict, disable, or prevent the use of nonessential services according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[a]	Implemented

Assessment Objective

Essential programs are defined

Program Procedure

The Cybersecurity Program Director defines programs essential to the organization according to the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team System Designer

Process Summary

- The Cybersecurity Program Director defines the organization's essential programs.
- The Govern Team documents the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents the essential programs in the System Catalog.

Process Evidence

Nonessential Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[b]	Implemented

Assessment Objective

The use of nonessential programs is defined

Program Procedure

The Cybersecurity Program Director defines the programs not essential to the organization for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team System Designer

Process Summary

- The Cybersecurity Program Director defines the organization's nonessential programs.
- The Govern Team documents the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents how nonessential programs are restricted in the System Catalog.

Process Evidence

Nonessential Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[c]	Implemented

Assessment Objective

The use of nonessential programs is restricted, disabled, or prevented as defined

Program Procedure

The System Deployer configures the system to restrict, disable, or prevent the use of nonessential programs according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Attack Surface Reduction Policy ASR-BlockMalCodeExecution-INT to block the use of malicious code
- Microsoft maintains its restriction of nonessential programs, functions, ports, protocols, and services in its datacenters by default.

Win 10/11 AVD

- Admins assigned to the "Virtual Machine Administrator Login" Role may perform local admin tasks on the AVD by default
- Configure Attack Surface Reduction Policy ASR-BlockMalCodeExecution-INT to block the use of malicious code
- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.
- Users assigned to the "Virtual Machine User Login" RBAC Role may sign and use the AVD, but may not use local admin permissions by default

Win 10/11 Win365

- Configure Attack Surface Reduction Policy ASR-BlockMalCodeExecution-INT to block the use of malicious code
- Configure CFG-ReplaceLocalAdmin-INT in Microsoft Intune to remove local administrator rights from users, and replace with select admins from Entra.
- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.

Configuration Evidence

ASR-BlockMalCodeExecution-INT
- Azure Admin Portal > Intune > Endpoint Security > Manage > Attack Surface Reduction

AVD RBAC Roles
- Azure > Resource Groups > [AVD Resource Group] > [Example AVD] > Access Control (IAM) > Role Assignments

CFG-ReplaceLocalAdmin-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Microsoft FedRAMP SSP
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

WCF-WebContentFiltering-DEF

- security.microsoft.us > system > settings > endpoints > rules > web content filtering

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[d]	Implemented

Assessment Objective
Essential functions are defined

Program Procedure
The Cybersecurity Program Director defines the functions essential to the organization for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team System Designer

Process Summary

- The Cybersecurity Program Director defines the organization's essential functions.
- The Govern Team documents the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents the essential functions in the System Catalog.

Process Evidence

Nonessential Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[e]	Implemented

Assessment Objective

The use of nonessential functions is defined

Program Procedure

The Cybersecurity Program Director defines the functions not essential to the organization for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team System Designer

Process Summary

- The Cybersecurity Program Director defines the organization's nonessential functions.
- The Govern Team documents the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents how nonessential functions are restricted in the System Catalog

Process Evidence

Nonessential Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[f]	Implemented

Assessment Objective

The use of nonessential functions is restricted, disabled, or prevented as defined

Program Procedure

The System Deployer configures the system to restrict, disable, or prevent the use of nonessential functions according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.
- Microsoft maintains its restriction of nonessential programs, functions, ports, protocols, and services in its datacenters by default.

Win 10/11 AVD

- Admins assigned to the “Virtual Machine Administrator Login” Role may perform local admin tasks on the AVD by default
- Configure "CFG-DisableCachedCredentials-INT" to disable storage of hashed credentials on Windows devices.
- Configure "CFG-DisableGuestAccount-INT" to disable the built-in Guest account on Windows devices.
- Configure "SCR-DisableAutoPlayForDefaultUserProfileOnWindowsDevices-INT" to disable Autoplay in the Default User Profile template on Windows devices.
- Configure "SCR-DisableWindowsAutoPlayOnWindowsDevices-INT" to disable Windows Explorer Autoplay on Windows devices.
- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.
- Users assigned to the “Virtual Machine User Login” RBAC Role may sign and use the AVD, but may not use local admin permissions by default

Win 10/11 Win365

- Configure "CFG-DisableCachedCredentials-INT" to disable storage of hashed credentials on Windows devices.
- Configure "CFG-DisableGuestAccount-INT" to disable the built-in Guest account on Windows devices.
- Configure "SCR-DisableAutoPlayForDefaultUserProfileOnWindowsDevices-INT" to disable Autoplay in the Default User Profile template on Windows devices.
- Configure "SCR-DisableWindowsAutoPlayOnWindowsDevices-INT" to disable Windows Explorer Autoplay on Windows devices.
- Configure CFG-ReplaceLocalAdmin-INT in Microsoft Intune to remove local administrator rights from users, and replace with select admins from Entra.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.

Configuration Evidence

AVD RBAC Roles
- Azure > Resource Groups > [AVD Resource Group] > [Example AVD] > Access Control (IAM) > Role Assignments

CFG-DisableCachedCredentials-INT
- Intune > Devices > Manage Devices > Configuration

CFG-DisableGuestAccount-INT
- Intune > Devices > Manage Devices > Configuration

CFG-ReplaceLocalAdmin-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Microsoft FedRAMP SSP
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Roles Defined in Entra PIM
- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

SCR-DisableWindowsAutoPlayOnWindowsDevices-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

SRC-DisableAutoPlayForDefaultUserProfileOnWindowsDevices-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

WCF-WebContentFiltering-DEF
- security.microsoft.us > system > settings > endpoints > rules > web content filtering

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[g]	Implemented

Assessment Objective

Essential ports are defined

Program Procedure

The Technical Lead defines the ports essential to the organization's IT operations for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team System Designer Technical Lead

Process Summary

- The Technical Lead defines the organization's essential ports.
- The Govern Team documents the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents the essential ports in the System Catalog.

Process Evidence

Nonessential Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[h]	Implemented

Assessment Objective

The use of nonessential ports is defined

Program Procedure

The Technical Lead defines the ports not essential to the organization's IT operations for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team System Designer Technical Lead

Process Summary

- The Technical Lead defines the organization's nonessential ports.
- The Govern Team documents the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents how nonessential ports are restricted in the System Catalog.

Process Evidence

Nonessential Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[i]	Implemented

Assessment Objective

The use of nonessential ports is restricted, disabled, or prevented as defined

Program Procedure

The System Deployer configures the system to restrict, disable, or prevent the use of nonessential ports according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft maintains its restriction of nonessential programs, functions, ports, protocols, and services in its datacenters by default.

Win 10/11 AVD

- Configure SCR-WinFirewallDenyByDefault-INT to deny inbound and outbound traffic by default.
- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.

Win 10/11 Win365

- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.

Configuration Evidence

Microsoft FedRAMP SSP
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

SCR-WinFirewallDenyByDefault-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

WCF-WebContentFiltering-DEF
- security.microsoft.us > system > settings > endpoints > rules > web content filtering

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[j]	Implemented

Assessment Objective

Essential protocols are defined

Program Procedure

The Technical Lead defines the protocols essential to the organization's IT operations for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team System Designer Technical Lead

Process Summary

- The Technical Lead defines the organization's essential protocols.
- The Govern Team documents the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents the essential protocols in the System Catalog.

Process Evidence

Nonessential Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[k]	Implemented

Assessment Objective

The use of nonessential protocols is defined

Program Procedure

The Technical Lead defines the protocols not essential to the organization's IT operations for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team System Designer Technical Lead

Process Summary

- The Technical Lead defines the organization's nonessential protocols.
- The Govern Team documents the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents how nonessential protocols are restricted in the System Catalog.

Process Evidence

Nonessential Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[l]	Implemented

Assessment Objective

The use of nonessential protocols is restricted, disabled, or prevented as defined

Program Procedure

The System Deployer configures the system to restrict, disable, or prevent the use of nonessential protocols according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft maintains its restriction of nonessential programs, functions, ports, protocols, and services in its datacenters by default.

Win 10/11 AVD

- Configure SCR-WinFirewallDenyByDefault-INT to deny inbound and outbound traffic by default.
- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.

Win 10/11 Win365

- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.

Configuration Evidence

Microsoft FedRAMP SSP
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

SCR-WinFirewallDenyByDefault-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

WCF-WebContentFiltering-DEF
- security.microsoft.us > system > settings > endpoints > rules > web content filtering

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[m]	Implemented

Assessment Objective

Essential services are defined

Program Procedure

The Technical Lead defines the services essential to the organization for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team System Designer Technical Lead

Process Summary

- The Technical Lead defines the organization's essential services.
- The Govern Team documents the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents the essential services in the System Catalog.

Process Evidence

Nonessential Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[n]	Implemented

Assessment Objective

The use of nonessential services is defined

Program Procedure

The Technical Lead defines the services not essential to the organization's IT operations for the Nonessential Functionality Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team System Designer Technical Lead

Process Summary

- The Technical Lead defines the organization's nonessential services.
- The Govern Team documents the Nonessential Functionality Section in the 3.4 Configuration Management Policy.
- The System Designer documents how nonessential services are restricted in the System Catalog.

Process Evidence

Nonessential Functionality Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.7[o]	Implemented

Assessment Objective

The use of nonessential services is restricted, disabled, or prevented as defined

Program Procedure

The System Deployer configures the system to restrict, disable, or prevent the use of nonessential services according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.
- Microsoft maintains its restriction of nonessential programs, functions, ports, protocols, and services in its datacenters by default.

Win 10/11 AVD

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.
- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.
- Deploy SCR-DisableNonessentialServices-INT platform script to block non-essential services on Windows endpoints.

Win 10/11 Win365

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.
- Configure WCF-WebContentFiltering-DEF to block inappropriate web content.
- Deploy SCR-DisableNonessentialServices-INT platform script to block non-essential services on Windows endpoints.

Configuration Evidence

CFG-VulnerabilityScans-INT
- Microsoft Defender Portal > Endpoints > Configuration Management > Endpoint Security Policies

Microsoft FedRAMP SSP
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

SCR-DisableNonessentialServices-INT
- Intune > Windows > Devices > Scripts and Remediations > Platform Scripts

WCF-WebContentFiltering-DEF
- security.microsoft.us > system > settings > endpoints > rules > web content filtering

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CM.L2-3.4.8		Application Execution Policy
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Procedure Summary

[a]	The Govern Team documents the denylist policy in the Application Execution Policy Section in the 3.4 Configuration Management Policy.
[b]	The Technical Lead documents software denied use under the denylist in the System Catalog.
[c]	The Harden Team configures the blocking of software.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.8[a]	Implemented

Assessment Objective

A policy specifying whether whitelisting or blacklisting is to be implemented is specified

Program Procedure

The Govern Team documents the denylist policy in the Application Execution Policy Section in the 3.4 Configuration Management Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents that the organization uses an denylist in the User, Process, and Asset Inventory Section in the 3.4 Configuration Management Policy.

Process Evidence

Application Execution Policy Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Assessment Objective Identifier	Assessment Objective Status
3.4.8[b]	Implemented

Assessment Objective
The software allowed to execute under whitelisting or denied use under blacklisting is specified

Program Procedure
The Technical Lead documents software denied use under the denylist in the System Catalog.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Technical Lead

Process Summary

- The Technical Lead documents the software denied use under the denylist in the System Catalog.

Process Evidence

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.8[c]	Implemented

Assessment Objective

Whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified

Program Procedure

The Harden Team configures the blocking of software.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

Win 10/11 AVD

- Admins assigned to the "Virtual Machine Administrator Login" Role may perform local admin tasks on the AVD by default
- Configure an App Control for Business policy ACP-SoftwareDenyListv1.1-INT to restrict the installation and execution of certain software.
- Users assigned to the "Virtual Machine User Login" RBAC Role may sign and use the AVD, but may not use local admin permissions by default

Win 10/11 Win365

- Configure an App Control for Business policy ACP-SoftwareDenyListv1.1-INT to restrict the installation and execution of certain software.
- Configure CFG-ReplaceLocalAdmin-INT in Microsoft Intune to remove local administrator rights from users, and replace with select admins from Entra.

Configuration Evidence

AVD RBAC Roles

- Azure > Resource Groups > [AVD Resource Group] > [Example AVD] > Access Control (IAM) > Role Assignments

CFG-ReplaceLocalAdmin-INT

- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Intune App Control for Business Policy

- Intune > Devices > Windows > Scripts and Remediations

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CM.L2-3.4.9		User-Installed Software
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Control and monitor user-installed software.

Procedure Summary

[a]	The Cybersecurity Program Director decides that a user install allowed policy is implemented to control the installation of software.
[b]	The System Deployer configures the system to prevent users from installing software on the denylist following the System Baseline Standard.
[c]	The System Security Analyst monitors for the unauthorized installation of software.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.9[a]	Implemented

Assessment Objective

A policy for controlling the installation of software by users is established

Program Procedure

The Cybersecurity Program Director decides that a user install allowed policy is implemented to control the installation of software.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team System Designer

Process Summary

- The Cybersecurity Program Director specifies that users are permitted to install software.
- The Govern Team documents that users are permitted to install software in the User-Installed Software Section in the 3.4 Configuration Management Policy.
- The System Designer develops the configuration to prevent users from installing unauthorized software.
- The System Designer documents the configuration to prevent users from installing software on the denylist in the System Baseline Standard.
- The System Designer develops the system to monitor for installation of software.
- The System Designer documents the configuration to monitor for the unauthorized installation of software in the System Baseline Standard.

Process Evidence

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

User-Installed Software Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.4 Configuration Management Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.9[b]	Implemented

Assessment Objective

Installation of software by users is controlled based on the established policy

Program Procedure

The System Deployer configures the system to prevent users from installing software on the denylist following the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.

Win 10/11 AVD

- Admins assigned to the “Virtual Machine Administrator Login” Role may perform local admin tasks on the AVD by default
- Configure an App Control for Business policy ACP-SoftwareDenyListv1.1-INT to restrict the installation and execution of certain software.
- Intune automatically adds Global Administrators, and privileged accounts with the "Microsoft Entra Joined Device Local Administrator" role to the local administrators group in Entra AD joined devices by default.
- Users assigned to the “Virtual Machine User Login” RBAC Role may sign and use the AVD, but may not use local admin permissions by default

Win 10/11 Win365

- Configure an App Control for Business policy ACP-SoftwareDenyListv1.1-INT to restrict the installation and execution of certain software.
- Configure CFG-ReplaceLocalAdmin-INT in Microsoft Intune to remove local administrator rights from users, and replace with select admins from Entra.
- Intune automatically adds Global Administrators, and privileged accounts with the "Microsoft Entra Joined Device Local Administrator" role to the local administrators group in Entra AD joined devices by default.

Configuration Evidence

AVD RBAC Roles

- Azure > Resource Groups > [AVD Resource Group] > [Example AVD] > Access Control (IAM) > Role Assignments

CFG-ReplaceLocalAdmin-INT

- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Intune App Control for Business Policy

- Intune > Devices > Windows > Scripts and Remediations

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Microsoft Entra Joined Device Local Administrator Article

- https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#microsoft-entra-joined-device-local-administrator

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.4.9[c]	Implemented

Assessment Objective

Installation of software by users is monitored

Program Procedure

The System Security Analyst monitors for the unauthorized installation of software.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default
- Microsoft reports on the installed software on endpoints by default.

Win 10/11 AVD

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Microsoft reports on the installed software on endpoints by default.

Win 10/11 Win365

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Microsoft reports on the installed software on endpoints by default.

Configuration Evidence

EDR-DeployDefenderConnector-INT
- Intune Portal > Endpoint Security > Endpoint Detection and Response

Microsoft Defender XDR to Sentinel Connector Learn Article
- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.1		Identification
SPRS Value	**SPRS Score**	**Practice Status**
5	5	Implemented

Practice Statement

Identify system users, processes acting on behalf of users, and devices.

Procedure Summary

[a]	The System Administrator identifies user account unique identifiers in the User, Process, and Asset Inventory.
[b]	The System Administrator identifies service principal unique identifiers in the User, Process, and Asset Inventory.
[c]	The System Administrator identifies device unique identifiers in the User, Process, and Asset Inventory.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.1[a]	Implemented

Assessment Objective

System users are identified

Program Procedure

The System Administrator identifies user account unique identifiers in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	System Administrator	Govern Team System Administrator

Process Summary

- The Govern Team documents the requirements for unique identifiers in the Identification Section in the 3.5 Identification and Authentication Policy.
- The System Administrator identifies authorized user accounts and their unique identifiers.
- The System Administrator documents authorized user accounts and their unique identifiers in the User, Process, and Asset Inventory.

Process Evidence

Identification Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.5 Identification and Authentication Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.1[b]	Implemented

Assessment Objective

Processes acting on behalf of users are identified

Program Procedure

The System Administrator identifies service principal unique identifiers in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	System Administrator	Govern Team System Administrator

Process Summary

- The Govern Team documents the requirements for unique identifiers in the Identification Section in the 3.5 Identification and Authentication Policy.
- The System Administrator identifies authorized service principals and their unique identifiers.
- The System Administrator documents authorized service principals and their unique identifiers in the User, Process, and Asset Inventory.

Process Evidence

Identification Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.5 Identification and Authentication Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.1[c]	Implemented

Assessment Objective

Devices accessing the system are identified

Program Procedure

The System Administrator identifies device unique identifiers in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	System Administrator	Govern Team System Administrator

Process Summary

- The Govern Team documents the requirements for unique identifiers in the Identification Section in the 3.5 Identification and Authentication Policy.
- The System Administrator identifies authorized devices and their unique identifiers.
- The System Administrator documents authorized devices and their unique identifiers in the User, Process, and Asset Inventory.

Process Evidence

Identification Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.5 Identification and Authentication Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.2		Authentication
SPRS Value	**SPRS Score**	**Practice Status**
5	5	Implemented

Practice Statement

Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Procedure Summary

[a]	The System Deployer configures the system such that user identities are authenticated according to the System Baseline Standard.
[b]	The System Deployer configures the system such that service principals are authenticated according to the System Baseline Standard.
[c]	The System Deployer configures the system such that devices are authenticated according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.2[a]	Implemented

Assessment Objective

The identity of each user is authenticated or verified as a prerequisite to system access

Program Procedure

The System Deployer configures the system such that user identities are authenticated according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Multifactor Authentication Methods in the Entra Portal

Win 10/11 AVD

- Configure "CFG-DisableCachedCredentials-INT" to disable storage of hashed credentials on Windows devices.
- Configure "CFG-DisableGuestAccount-INT" to disable the built-in Guest account on Windows devices.
- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares
- Configure CAP-RequireMFAEachSigninToAVD-EID to require users to provide authentication each sign-in to the AVD.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure "CFG-DisableCachedCredentials-INT" to disable storage of hashed credentials on Windows devices.
- Configure "CFG-DisableGuestAccount-INT" to disable the built-in Guest account on Windows devices.
- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireMFAEachSigninToAVD-EID
- Entra Admin Portal > Security > Conditional Access

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

CFG-DisableCachedCredentials-INT
- Intune > Devices > Manage Devices > Configuration

CFG-DisableGuestAccount-INT
- Intune > Devices > Manage Devices > Configuration

CFG-DisallowNullSessions-INT
- Intune > Devices > Manage Devices > Configuration

Entra Authentication Methods Screenshot
- Entra Portal > Protection > Authentication Methods > Manage > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.2[b]	Implemented

Assessment Objective

The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access

Program Procedure

The System Deployer configures the system such that service principals are authenticated according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Client Secrets for Service Principals

Win 10/11 AVD

- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares
- Configure CAP-RequireMFAEachSigninToAVD-EID to require users to provide authentication each sign-in to the AVD.

Win 10/11 Win365

- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares

Configuration Evidence

CAP-RequireMFAEachSigninToAVD-EID

- Entra Admin Portal > Security > Conditional Access

CFG-DisallowNullSessions-INT

- Intune > Devices > Manage Devices > Configuration

Example App Registration Client Secret

- Azure > App Registrations > Example App > Manage > Certificates and Secrets > Client Secrets

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.2[c]	Implemented

Assessment Objective

The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access

Program Procedure

The System Deployer configures the system such that devices are authenticated according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Multifactor Authentication Methods in the Entra Portal

Win 10/11 AVD

- Configure CAP-RequireMFAEachSigninToAVD-EID to require users to provide authentication each sign-in to the AVD.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireMFAEachSigninToAVD-EID
- Entra Admin Portal > Security > Conditional Access

Entra Authentication Methods Screenshot
- Entra Portal > Protection > Authentication Methods > Manage > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.3		Multifactor Authentication
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Procedure Summary

[a]	The Technical Lead ensures Privileged User Accounts are identified in the User, Process, and Asset Inventory.
[b]	The System Deployer implements MFA for local access to privileged accounts.
[c]	The System Deployer implements MFA for network access to privileged accounts.
[d]	The System Deployer implements MFA for network access to non-privileged accounts.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.3[a]	Implemented

Assessment Objective

Privileged accounts are identified

Program Procedure

The Technical Lead ensures Privileged User Accounts are identified in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team System Administrator System Deployer System Designer

Process Summary

- The Govern Team documents the requirements for multifactor authentication in the Multifactor Authentication (MFA) Section.
- The System Designer defines the configuration for multifactor authentication.
- The System Designer documents the configuration for multifactor authentication in the System Baseline Standard.
- The System Deployer configures systems such that multifactor authentication is implemented according to the System Baseline Standard.
- The System Administrator identifies privileged identities that belong to the privileged users.
- The System Administrator documents privileged identities on the User, Process, and Asset Inventory.

Process Evidence

Multifactor Authentication (MFA) Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.5 Identification and Authentication Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.3[b]	Implemented

Assessment Objective

Multifactor authentication is implemented for local access to privileged accounts

Program Procedure

The System Deployer implements MFA for local access to privileged accounts.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-RequireMFADeviceEnrollment-EID to require multifactor authentication for device enrollment
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.

Win 10/11 AVD

- Configure CAP-RequireMFAEachSigninToAVD-EID to require users to provide authentication each sign-in to the AVD.
- Configure the group "GRP-ArdalystHardenPIM-EID" with the role "Microsoft Entra Joined Device Local Administrator" role. These administrators cannot access devices without first using multifactor authentication through the tenant.
- Intune automatically adds Global Administrators, and privileged accounts with the "Microsoft Entra Joined Device Local Administrator" role to the local administrators group in Entra AD joined devices by default.

Win 10/11 Win365

- Configure the group "GRP-ArdalystHardenPIM-EID" with the role "Microsoft Entra Joined Device Local Administrator" role. These administrators cannot access devices without first using multifactor authentication through the tenant.
- Intune automatically adds Global Administrators, and privileged accounts with the "Microsoft Entra Joined Device Local Administrator" role to the local administrators group in Entra AD joined devices by default.

Configuration Evidence

CAP-RequireMFADeviceEnrollment-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireMFAEachSigninToAVD-EID
- Entra Admin Portal > Security > Conditional Access

GRP-ArdalystHardenPIM-EID
- Azure > Entra > Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Microsoft Entra Joined Device Local Administrator Article

- https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#microsoft-entra-joined-device-local-administrator

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.3[c]	Implemented

Assessment Objective

Multifactor authentication is implemented for network access to privileged accounts

Program Procedure

The System Deployer implements MFA for network access to privileged accounts.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Conditional Access Policy CAP-RequireMFADeviceEnrollment-EID to require multifactor authentication for device enrollment
- Configure Multifactor Authentication Methods in the Entra Portal
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.

Win 10/11 AVD

- Configure CAP-RequireMFAEachSigninToAVD-EID to require users to provide authentication each sign-in to the AVD.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireMFADeviceEnrollment-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireMFAEachSigninToAVD-EID
- Entra Admin Portal > Security > Conditional Access

Entra Authentication Methods Screenshot
- Entra Portal > Protection > Authentication Methods > Manage > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.3[d]	Implemented

Assessment Objective

Multifactor authentication is implemented for network access to non-privileged accounts

Program Procedure

The System Deployer implements MFA for network access to non-privileged accounts.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Conditional Access Policy CAP-RequireMFADeviceEnrollment-EID to require multifactor authentication for device enrollment
- Configure Multifactor Authentication Methods in the Entra Portal

Win 10/11 AVD

- Configure CAP-RequireMFAEachSigninToAVD-EID to require users to provide authentication each sign-in to the AVD.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireMFADeviceEnrollment-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireMFAEachSigninToAVD-EID
- Entra Admin Portal > Security > Conditional Access

Entra Authentication Methods Screenshot
- Entra Portal > Protection > Authentication Methods > Manage > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.4		Replay-Resistant Authentication
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

Procedure Summary

[a]	The System Designer configures each system to employ Replay-Resistant Authentication methods.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.4[a]	Implemented

Assessment Objective

Replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts

Program Procedure

The System Designer configures each system to employ Replay-Resistant Authentication methods.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 AVD

- Configure CAP-RequireMFAEachSigninToAVD-EID to require users to provide authentication each sign-in to the AVD.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID

- Entra Admin Portal > Security > Conditional Access

CAP-RequireMFAEachSigninToAVD-EID

- Entra Admin Portal > Security > Conditional Access

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.5		Identifier Reuse
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Prevent reuse of identifiers for a defined period.

Procedure Summary

[a]	The Govern Team documents that identifiers can never be reused in the Identifier Reuse Section in the 3.5 Identification and Authentication Policy.
[b]	The System Deployer configures the system such that identifiers cannot be reused according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.5[a]	Implemented

Assessment Objective

A period within which identifiers cannot be reused is defined

Program Procedure

The Govern Team documents that identifiers can never be reused in the Identifier Reuse Section in the 3.5 Identification and Authentication Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team System Designer

Process Summary

- The Govern Team documents that identifiers cannot be reused indefinitely in the Identifier Reuse Section in the 3.5 Identification and Authentication Policy.
- The System Designer develops the configuration preventing the reuse of identifiers.
- The System Designer documents the configuration preventing the reuse of identifiers in the System Baseline Standard.

Process Evidence

Identifier Reuse Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.5 Identification and Authentication Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.5[b]	Implemented

Assessment Objective

Reuse of identifiers is prevented within the defined period

Program Procedure

The System Deployer configures the system such that identifiers cannot be reused according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft provides globally unique identifiers (GUIDs) for all user, group, device objects by default.

Win 10/11 AVD

- Microsoft provides globally unique identifiers (GUIDs) for all user, group, device objects by default.

Win 10/11 Win365

- Microsoft provides globally unique identifiers (GUIDs) for all user, group, device objects by default.

Configuration Evidence

Microsoft CMMC Additional Controls Learn Article

- https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-additional-controls

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.6		Identifier Handling
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Disable identifiers after a defined period of inactivity.

Procedure Summary

[a]	The Govern Team defines a period of inactivity after which an identifier is disabled and documents in the Identifier Handling Section in the 3.5 Identification and Authentication Policy.
[b]	The System Deployer configures the system such that identifiers are disabled after sixty (60) days according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.6[a]	Implemented

Assessment Objective

A period of inactivity after which an identifier is disabled is defined

Program Procedure

The Govern Team defines a period of inactivity after which an identifier is disabled and documents in the Identifier Handling Section in the 3.5 Identification and Authentication Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director defines the period of inactivity after which an identifier is disabled is sixty (60) days.
- The Govern Team documents a period of inactivity after which an identifier is disabled in the Identifier Handling Section in the 3.5 Identification and Authentication Policy.
- The Cybersecurity Program Director identifies that privileged user accounts that are exempt from the defined period of inactivity.
- The Govern Team documents the privileged user accounts that are exempt from the period of inactivity policy in the Identifier Handling Section.

Process Evidence

Identifier Handling Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.5 Identification and Authentication Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.6[b]	Implemented

Assessment Objective

Identifiers are disabled after the defined period of inactivity

Program Procedure

The System Deployer configures the system such that identifiers are disabled after sixty (60) days according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Azure Workbook AZW-StaleAccounts-AZR to monitor for stale accounts.

Configuration Evidence

AZW-StaleAccounts-AZR

- Azure Admin Console > Azure Workbooks

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.7		Password Complexity
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Enforce a minimum password complexity and change of characters when new passwords are created.

Procedure Summary

[a]	The Govern Team documents password complexity requirements in the Password Complexity Section in the 3.5 Identification and Authentication Policy.
[b]	The Govern Team documents password complexity requirements in the Password Complexity Section in the 3.5 Identification and Authentication Policy.
[c]	The System Deployer configures the system such that password complexity requirements are enforced according to the System Baseline Standard.
[d]	The System Deployer configures the system such that password change of character requirements are enforced according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.7[a]	Implemented

Assessment Objective
Password complexity requirements are defined

Program Procedure
The Govern Team documents password complexity requirements in the Password Complexity Section in the 3.5 Identification and Authentication Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents password complexity requirements in the Password Complexity Section in the 3.5 Identification and Authentication Policy.

Process Evidence

Password Complexity Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.5 Identification and Authentication Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.7[b]	Implemented

Assessment Objective
Password change of character requirements are defined

Program Procedure
The Govern Team documents password complexity requirements in the Password Complexity Section in the 3.5 Identification and Authentication Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents password change of character requirements in the Password Complexity Section in the 3.5 Identification and Authentication Policy.

Process Evidence

Password Complexity Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.5 Identification and Authentication Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.7[c]	Implemented

Assessment Objective

Minimum password complexity requirements as defined are enforced when new passwords are created

Program Procedure

The System Deployer configures the system such that password complexity requirements are enforced according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft requires passwords to be at least 8 characters long, and include three of the following: (uppercase letters, lowercase letters, numbers, symbols) by default

Win 10/11 AVD

- Microsoft requires passwords to be at least 8 characters long, and include three of the following: (uppercase letters, lowercase letters, numbers, symbols) by default

Win 10/11 Win365

- Microsoft requires passwords to be at least 8 characters long, and include three of the following: (uppercase letters, lowercase letters, numbers, symbols) by default

Configuration Evidence

Password policies and account restrictions in Microsoft Entra ID

- https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.7[d]	Implemented

Assessment Objective

Minimum password change of character requirements as defined are enforced when new passwords are created

Program Procedure

The System Deployer configures the system such that password change of character requirements are enforced according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft requires passwords to be at least 8 characters long, and include three of the following: (uppercase letters, lowercase letters, numbers, symbols) by default

Win 10/11 AVD

- Microsoft requires passwords to be at least 8 characters long, and include three of the following: (uppercase letters, lowercase letters, numbers, symbols) by default

Win 10/11 Win365

- Microsoft requires passwords to be at least 8 characters long, and include three of the following: (uppercase letters, lowercase letters, numbers, symbols) by default

Configuration Evidence

Password policies and account restrictions in Microsoft Entra ID

- https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.8		Password Reuse
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Prohibit password reuse for a specified number of generations.

Procedure Summary

[a]	The Govern Team defines that passwords may not be reused for no less than one (1) generation in the Password Reuse Section in the 3.5 Identification and Authentication Policy.
[b]	The System Deployer configures systems such that they may not reuse, at a minimum, the previous password according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.8[a]	Implemented

Assessment Objective

The number of generations during which a password cannot be reused is specified

Program Procedure

The Govern Team defines that passwords may not be reused for no less than one (1) generation in the Password Reuse Section in the 3.5 Identification and Authentication Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents that passwords may not be reused for one generation in the Password Reuse Section in the 3.5 Identification and Authentication Policy.

Process Evidence

Password Reuse Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.5 Identification and Authentication Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.8[b]	Implemented

Assessment Objective

Reuse of passwords is prohibited during the specified number of generations

Program Procedure

The System Deployer configures systems such that they may not reuse, at a minimum, the previous password according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft restricts password reuse to only prevent the reuse of the previously set password. This is set by default and cannot be changed.

Win 10/11 AVD

- Microsoft restricts password reuse to only prevent the reuse of the previously set password. This is set by default and cannot be changed.

Win 10/11 Win365

- Microsoft restricts password reuse to only prevent the reuse of the previously set password. This is set by default and cannot be changed.

Configuration Evidence

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.9		Temporary Passwords
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Allow temporary password use for system logons with an immediate change to a permanent password.

Procedure Summary

[a]	The System Deployer configures the system to enforce the immediate change of a temporary password for system logon, according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.9[a]	Implemented

Assessment Objective

An immediate change to a permanent password is required when a temporary password is used for system logon

Program Procedure

The System Deployer configures the system to enforce the immediate change of a temporary password for system logon, according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft Entra enforces temporary password reset by default

Win 10/11 AVD

- Microsoft Entra enforces temporary password reset by default

Win 10/11 Win365

- Microsoft Entra enforces temporary password reset by default

Configuration Evidence

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.10		Cryptographically-Protected Passwords
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Store and transmit only cryptographically-protected passwords.

Procedure Summary

[a]	The Govern Team determines systems where the vendor does not provide cryptographically-protected passwords are not permitted in the environment and documents in the Cryptographically-Protected Passwords Section in the 3.5 Identification and Authentication Policy.
[b]	The System Deployer configures systems to transmit only cryptographically protected passwords according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.10[a]	Implemented

Assessment Objective

Passwords are cryptographically protected in storage

Program Procedure

The Govern Team determines systems where the vendor does not provide cryptographically-protected passwords are not permitted in the environment and documents in the Cryptographically-Protected Passwords Section in the 3.5 Identification and Authentication Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team System Designer Technical Lead

Process Summary

- The Technical Lead determines that systems that do not provide cryptographically protected passwords are not permitted.
- The Govern Team defines that passwords must not be transmitted unless they are cryptographically protected.
- The Govern Team documents the organization's policy regarding cryptographic protection of passwords in the Cryptographically-Protected Passwords Section in the 3.5 Identification and Authentication Policy.
- The System Designer verifies that all systems in the environment provide cryptographically-protected passwords and documents in the System Baseline Standard.

Process Evidence

Cryptographically-Protected Passwords Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.5 Identification and Authentication Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.10[b]	Implemented

Assessment Objective

Passwords are cryptographically protected in transit

Program Procedure

The System Deployer configures systems to transmit only cryptographically protected passwords according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Ardalyst stores breakglass passwords in a FIPS validated Keeper Security Government Cloud instance. Access to breakglass passwords is limited to a subset of privileged users, requires MFA, and is audited.
- Microsoft provides an email encryption tool by default.

Win 10/11 AVD

- Ardalyst stores breakglass passwords in a FIPS validated Keeper Security Government Cloud instance. Access to breakglass passwords is limited to a subset of privileged users, requires MFA, and is audited.
- Microsoft provides an email encryption tool by default.

Win 10/11 Win365

- Ardalyst stores breakglass passwords in a FIPS validated Keeper Security Government Cloud instance. Access to breakglass passwords is limited to a subset of privileged users, requires MFA, and is audited.
- Microsoft provides an email encryption tool by default.

Configuration Evidence

Keeper Password Management (Third-Party)

- https://www.keepersecurity.com/ > Customer Breakglass Vaults > Client's Vault

Microsoft Email Encryption Learn Article

- https://learn.microsoft.com/en-us/purview/ome

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IA.L2-3.5.11		Obscure Feedback
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Obscure feedback of authentication information.

Procedure Summary

[a]	The System Deployer configures the system such that the authentication information is obscured during the authentication process according to the Obscure Feedback Section in the 3.5 Identification and Authentication Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.5.11[a]	Implemented

Assessment Objective

Authentication information is obscured during the authentication process

Program Procedure

The System Deployer configures the system such that the authentication information is obscured during the authentication process according to the Obscure Feedback Section in the 3.5 Identification and Authentication Policy.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft Entra obscures all authentication feedback by default

Win 10/11 AVD

- Microsoft Windows obscures all authentication feedback by default

Win 10/11 Win365

- Microsoft Windows obscures all authentication feedback by default

Configuration Evidence

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Microsoft Web Documentation Ref: CMMC IA Controls

- https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-identification-and-authentication

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IR.L2-3.6.1		Incident Handling
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Procedure Summary

[a]	The Govern Team establishes an operational incident-handling capability in the Incident Response Plan according to the Incident Handling Section in the 3.6 Incident Response Policy.
[b]	The Govern Team includes an incident preparation procedure in the Incident Response Plan.
[c]	The Govern Team includes an incident detection procedure in the Incident Response Plan.
[d]	The Govern Team includes an incident analysis procedure in the Incident Response Plan.
[e]	The Govern Team includes an incident containment procedure in the Incident Response Plan.
[f]	The Govern Team includes an incident recovery procedure in the Incident Response Plan.
[g]	The Govern Team includes user response activities and procedures in the Incident Response Plan.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.1[a]	Implemented

Assessment Objective

An operational incident-handling capability is established

Program Procedure

The Govern Team establishes an operational incident-handling capability in the Incident Response Plan according to the Incident Handling Section in the 3.6 Incident Response Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team Operate Team

Process Summary

- The Govern Team documents the Incident Handling Section in the 3.6 Incident Response Policy.
- The Govern Team drafts the Incident Response Plan.
- The Cybersecurity Program Director reviews the Incident Response Plan.
- The Cybersecurity Program Director accepts the Incident Response Plan.
- The Cybersecurity Program Director assigns members of the organization to the Incident Response Team (IRT) in the Roles & Responsibilities Section of the System Security Plan.
- The Operate Team documents the members assigned to the IRT in the Roles & Responsibilities Section of the System Security Plan.

Process Evidence

Incident Handling Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.6 Incident Response Policy

Incident Response Plan
- SharePoint > Govern Docs > Artifacts > Incident Response Plan

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.1[b]	Implemented

Assessment Objective

The operational incident-handling capability includes preparation

Program Procedure

The Govern Team includes an incident preparation procedure in the Incident Response Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team Operate Team

Process Summary

- The Govern Team documents the Incident Handling Section in the 3.6 Incident Response Policy.
- The Govern Team drafts the Incident Response Plan.
- The Cybersecurity Program Director reviews the Incident Response Plan.
- The Cybersecurity Program Director accepts the Incident Response Plan.
- The Cybersecurity Program Director assigns members of the organization to the Incident Response Team (IRT) in the Roles & Responsibilities Section of the System Security Plan.
- The Operate Team documents the members assigned to the IRT in the Roles & Responsibilities Section of the System Security Plan.

Process Evidence

Incident Handling Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.6 Incident Response Policy

Incident Response Plan
- SharePoint > Govern Docs > Artifacts > Incident Response Plan

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.1[c]	Implemented

Assessment Objective

The operational incident-handling capability includes detection

Program Procedure

The Govern Team includes an incident detection procedure in the Incident Response Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team Operate Team

Process Summary

- The Govern Team documents the Incident Handling Section in the 3.6 Incident Response Policy.
- The Govern Team drafts the Incident Response Plan.
- The Cybersecurity Program Director reviews the Incident Response Plan.
- The Cybersecurity Program Director accepts the Incident Response Plan.
- The Cybersecurity Program Director assigns members of the organization to the Incident Response Team (IRT) in the Roles & Responsibilities Section of the System Security Plan.
- The Operate Team documents the members assigned to the IRT in the Roles & Responsibilities Section of the System Security Plan.

Process Evidence

Incident Handling Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.6 Incident Response Policy

Incident Response Plan
- SharePoint > Govern Docs > Artifacts > Incident Response Plan

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.1[d]	Implemented

Assessment Objective

The operational incident-handling capability includes analysis

Program Procedure

The Govern Team includes an incident analysis procedure in the Incident Response Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team Operate Team

Process Summary

- The Govern Team documents the Incident Handling Section in the 3.6 Incident Response Policy.
- The Govern Team drafts the Incident Response Plan.
- The Cybersecurity Program Director reviews the Incident Response Plan.
- The Cybersecurity Program Director accepts the Incident Response Plan.
- The Cybersecurity Program Director assigns members of the organization to the Incident Response Team (IRT) in the Roles & Responsibilities Section of the System Security Plan.
- The Operate Team documents the members assigned to the IRT in the Roles & Responsibilities Section of the System Security Plan.

Process Evidence

Incident Handling Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.6 Incident Response Policy

Incident Response Plan
- SharePoint > Govern Docs > Artifacts > Incident Response Plan

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.1[e]	Implemented

Assessment Objective

The operational incident-handling capability includes containment

Program Procedure

The Govern Team includes an incident containment procedure in the Incident Response Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team Operate Team

Process Summary

- The Govern Team documents the Incident Handling Section in the 3.6 Incident Response Policy.
- The Govern Team drafts the Incident Response Plan.
- The Cybersecurity Program Director reviews the Incident Response Plan.
- The Cybersecurity Program Director accepts the Incident Response Plan.
- The Cybersecurity Program Director assigns members of the organization to the Incident Response Team (IRT) in the Roles & Responsibilities Section of the System Security Plan.
- The Operate Team documents the members assigned to the IRT in the Roles & Responsibilities Section of the System Security Plan.

Process Evidence

Incident Handling Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.6 Incident Response Policy

Incident Response Plan
- SharePoint > Govern Docs > Artifacts > Incident Response Plan

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.1[f]	Implemented

Assessment Objective

The operational incident-handling capability includes recovery

Program Procedure

The Govern Team includes an incident recovery procedure in the Incident Response Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team Operate Team

Process Summary

- The Govern Team documents the Incident Handling Section in the 3.6 Incident Response Policy.
- The Govern Team drafts the Incident Response Plan.
- The Cybersecurity Program Director reviews the Incident Response Plan.
- The Cybersecurity Program Director accepts the Incident Response Plan.
- The Cybersecurity Program Director assigns members of the organization to the Incident Response Team (IRT) in the Roles & Responsibilities Section of the System Security Plan.
- The Operate Team documents the members assigned to the IRT in the Roles & Responsibilities Section of the System Security Plan.

Process Evidence

Incident Handling Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.6 Incident Response Policy

Incident Response Plan
- SharePoint > Govern Docs > Artifacts > Incident Response Plan

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.1[g]	Implemented

Assessment Objective

The operational incident-handling capability includes user response activities

Program Procedure

The Govern Team includes user response activities and procedures in the Incident Response Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team Operate Team

Process Summary

- The Govern Team documents the Incident Handling Section in the 3.6 Incident Response Policy.
- The Govern Team drafts the Incident Response Plan.
- The Cybersecurity Program Director reviews the Incident Response Plan.
- The Cybersecurity Program Director accepts the Incident Response Plan.
- The Cybersecurity Program Director assigns members of the organization to the Incident Response Team (IRT) in the Roles & Responsibilities Section of the System Security Plan.
- The Operate Team documents the members assigned to the IRT in the Roles & Responsibilities Section of the System Security Plan.

Process Evidence

Incident Handling Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.6 Incident Response Policy

Incident Response Plan
- SharePoint > Govern Docs > Artifacts > Incident Response Plan

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IR.L2-3.6.2		Incident Reporting
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Procedure Summary

[a]	The Defend Team tracks incidents via an Incident Response Case according to the Incident Reporting Section in the 3.6 Incident Response Policy.
[b]	The Defend Team documents the incident in an Incident Response Case and submits through the support portal.
[c]	The Cybersecurity Program Director identifies the authorities to whom incidents are to be reported to and documents them in the User, Process, and Asset Inventory.
[d]	The Cybersecurity Program Director identifies the organizational official to whom incidents are to be reported to and documents them in the User, Process, and Asset Inventory.
[e]	The Cybersecurity Program Director notifies the identified authorities of incidents.
[f]	The Defend Team notifies the identified organizational officials of incidents via the Incident Response Case in the support portal.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.2[a]	Implemented

Assessment Objective

Incidents are tracked

Program Procedure

The Defend Team tracks incidents via an Incident Response Case according to the Incident Reporting Section in the 3.6 Incident Response Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Defend Team	Cybersecurity Program Director Defend Team Govern Team

Process Summary

- The Govern Team documents the Incident Reporting Section in the 3.6 Incident Response Policy.
- The Defend Team opens an Event Investigation Case based on system alert and/or advisories.
- The Defend Team performs analysis on the Event Investigation Case to determine a response.
- The Defend Team documents the analysis of the Event Investigation Case.
- The Cybersecurity Program Director reviews the Event Investigation Case.
- The Cybersecurity Program Director determines if the event is an incident.
- The Cybersecurity Program Director initiates the Incident Response Plan.

Process Evidence

Event Investigation Case
- support.ardalyst.com

Incident Reporting Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.6 Incident Response Policy

Incident Response Plan
- SharePoint > Govern Docs > Artifacts > Incident Response Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Assessment Objective Identifier	Assessment Objective Status
3.6.2[b]	Implemented

Assessment Objective

Incidents are documented

Program Procedure

The Defend Team documents the incident in an Incident Response Case and submits through the support portal.

Procedure Type	Responsible Role	Supporting Roles
Process	Defend Team	Cybersecurity Program Director Defend Team Govern Team

Process Summary

- The Govern Team documents the Incident Reporting Section in the 3.6 Incident Response Policy.
- For incidents, the Defend Team converts the Event Investigation Case into an Incident Response Case.
- The Defend Team documents the analysis of incident in the Incident Response Case.
- The Cybersecurity Program Director determines if incident is reportable.
- The Cybersecurity Program Director initiates the Incident Response Plan.

Process Evidence

Incident Reporting Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.6 Incident Response Policy

Incident Response Case
- support.ardalyst.com

Incident Response Plan
- SharePoint > Govern Docs > Artifacts > Incident Response Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.2[c]	Implemented

Assessment Objective

Authorities to whom incidents are to be reported are identified

Program Procedure

The Cybersecurity Program Director identifies the authorities to whom incidents are to be reported to and documents them in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Operate Team

Process Summary

- The Cybersecurity Program Director identifies the authorities to whom incidents are reported to.
- The Operate Team documents authorities to whom incidents are reported to in the User, Process, and Asset Inventory.

Process Evidence

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.2[d]	Implemented

Assessment Objective

Organizational officials to whom incidents are to be reported are identified

Program Procedure

The Cybersecurity Program Director identifies the organizational official to whom incidents are to be reported to and documents them in the User, Process, and Asset Inventory.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Operate Team

Process Summary

- The Cybersecurity Program Director identifies organizational officials to whom incidents are reported to.
- The Operate Team documents organizational officials to whom incidents are reported to in the User, Process, and Asset Inventory.

Process Evidence

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.2[e]	Implemented

Assessment Objective

Identified authorities are notified of incidents

Program Procedure

The Cybersecurity Program Director notifies the identified authorities of incidents.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director

Process Summary

- The Cybersecurity Program Director determines if incident is reportable.
- The Cybersecurity Program Director notifies authorities of an incident based on reporting parties identified in the User, Process, and Asset Inventory.

Process Evidence

Incident Response Case
- support.ardalyst.com

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.2[f]	Implemented

Assessment Objective
Identified organizational officials are notified of incidents

Program Procedure
The Defend Team notifies the identified organizational officials of incidents via the Incident Response Case in the support portal.

Procedure Type	Responsible Role	Supporting Roles
Process	Defend Team	Cybersecurity Program Director Defend Team

Process Summary

- The Cybersecurity Program Director determines if incident is reportable.
- The Defend Team notifies the identified organization officials of incidents via the Incident Response Case in the support portal.

Process Evidence

Incident Response Case
- support.ardalyst.com

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
IR.L2-3.6.3		Incident Response Testing
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement
Test the organizational incident response capability.

Procedure Summary	
[a]	The Govern Team tests organizational incident response capabilities through tabletop exercises according to the Incident Response Testing Section in the 3.6 Incident Response Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.6.3[a]	Implemented

Assessment Objective

The incident response capability is tested

Program Procedure

The Govern Team tests organizational incident response capabilities through tabletop exercises according to the Incident Response Testing Section in the 3.6 Incident Response Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team Incident Response Team

Process Summary

- The Govern Team documents requirements for the tabletop exercise in the Incident Response Testing Section in the 3.6 Incident Response Policy.
- The Cybersecurity Program Director schedules working session for Tabletop Exercise in the Tesseract Calendar.
- The Govern Team drafts the Tabletop Exercise.
- The Govern Team conducts the Tabletop Exercise with Incident Response Team.
- The Incident Response Team documents findings from the exercise in the Tabletop Exercise.
- If the Incident Response Team identifies updates to the Incident Response Plan, the Govern Team opens a Change Control Request Case to implement the updates.

Process Evidence

Change Control Request Case
- support.ardalyst.com

Incident Response Testing Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.6 Incident Response Policy

Tabletop Exercise
- SharePoint > Govern Docs > Artifacts > Tabletop Exercise

Tesseract Calendar
- SharePoint > Govern Docs > Artifacts > Tesseract Calendar

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MA.L2-3.7.1		Perform Maintenance
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Perform maintenance on organizational systems.

Procedure Summary

[a]	The System Maintainer performs system maintenance according to the Perform Maintenance Section in the 3.7 Maintenance Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.7.1[a]	Implemented

Assessment Objective

System maintenance is performed

Program Procedure

The System Maintainer performs system maintenance according to the Perform Maintenance Section in the 3.7 Maintenance Policy.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Escalation Support Team Harden Team	Escalation Support Team Harden Team

Configuration Summary

M365 GCC-H

- After connectors are set up, Defender XDR audits all cloud operations by default. Each audit log entry contains a user's immutable objectID that can be used to uniquely trace an individual system user to each action.
- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Qualys

- A Qualys Patch Management Agent is deployed to scan for, and automatically remediate vulnerabilities via patches made available by vendors.

Win 10/11 AVD

- Configure an Automation Account within Azure to start AVDs on Friday morning for patch cycle.
- Configure CFG-AVDWindowsUpdateForBusiness-INT to implement forced updates on AVD.
- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.
- Configure Device Cleanup Rule DCU-DeviceCleanUp-INT to remove devices after 30 days without check-in.
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.

Win 10/11 Win365

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.
- Configure Device Cleanup Rule DCU-DeviceCleanUp-INT to remove devices after 30 days without check-in.
- Configure Windows Update Ring WUR-WindowsUpdateRing-INT to enforce Windows updates on managed endpoints
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.

Configuration Evidence

Automation Account for Patch

- Azure portal > Automation Account

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

CFG-AVDWindowsUpdateForBusiness-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-VulnerabilityScans-INT
- Microsoft Defender Portal > Endpoints > Configuration Management > Endpoint Security Policies

DCU-DeviceCleanUp-INT
- Intune > Home > Devices > Device Clean-Up Rules > Create

Microsoft CMMC Additional Controls Learn Article
- https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-additional-controls

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Qualys Agent Dashboard
- Qualys > Agent Dashboard

WUR-WindowsUpdateRing-INT
- Intune Portal > Devices > Management > Windows Updates

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MA.L2-3.7.2		System Maintenance Control
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Procedure Summary

[a]	The System Deployer configures the system such that tools used to conduct system maintenance are controlled according to the System Baseline Standard.
[b]	The System Deployer configures the system such that techniques used to conduct system maintenance are controlled according to the System Baseline Standard.
[c]	The System Deployer configures the system such that mechanisms used to conduct system maintenance are controlled according to the System Baseline Standard.
[d]	The System Deployer configures the system such that personnel used to conduct system maintenance are controlled according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.7.2[a]	Implemented

Assessment Objective

Tools used to conduct system maintenance are controlled

Program Procedure

The System Deployer configures the system such that tools used to conduct system maintenance are controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Multifactor Authentication Methods in the Entra Portal
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.

Win 10/11 AVD

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID

- Entra Admin Portal > Security > Conditional Access

Entra Authentication Methods Screenshot

- Entra Portal > Protection > Authentication Methods > Manage > Policies

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.7.2[b]	Implemented

Assessment Objective

Techniques used to conduct system maintenance are controlled

Program Procedure

The System Deployer configures the system such that techniques used to conduct system maintenance are controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.

Win 10/11 AVD

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID

- Entra Admin Portal > Security > Conditional Access

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles

or

Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.7.2[c]	Implemented

Assessment Objective

Mechanisms used to conduct system maintenance are controlled

Program Procedure

The System Deployer configures the system such that mechanisms used to conduct system maintenance are controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.

Win 10/11 AVD

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID

- Entra Admin Portal > Security > Conditional Access

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.7.2[d]	Implemented

Assessment Objective

Personnel used to conduct system maintenance are controlled

Program Procedure

The System Deployer configures the system such that personnel used to conduct system maintenance are controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.

Win 10/11 AVD

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID

- Entra Admin Portal > Security > Conditional Access

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MA.L2-3.7.3		Equipment Sanitization
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Ensure equipment removed for off-site maintenance is sanitized of any CUI.

Procedure Summary

[a]	The Govern Team documents equipment containing CUI is not permitted in the environment.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.7.3[a]	Implemented

Assessment Objective
Equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI

Program Procedure
The Govern Team documents equipment containing CUI is not permitted in the environment.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents that equipment containing CUI is not permitted in the Equipment Sanitization Section in the 3.7 Maintenance Policy.

Process Evidence

Equipment Sanitization Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.7 Maintenance Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MA.L2-3.7.4		Media Inspection
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

Procedure Summary

[a]	The System Deployer configures the system such that removable media is not allowed according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.7.4[a]	Implemented

Assessment Objective

Media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI

Program Procedure

The System Deployer configures the system such that removable media is not allowed according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

Win 10/11 AVD

- Configure CFG-BlockAVDDriveRedirection-INT to block drive redirection to client endpoints from AVD sessions.
- Configure CFG-BlockAVDUSBDriveRedirection-INT to block AVD drive redirection to client endpoints from AVD sessions

Win 10/11 Win365

- Configure CFG-BlockW365DriveRedirection-INT to block drive redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365USBDriveRedirection-INT to block USB drive redirection to client endpoints from W365 sessions

Configuration Evidence

CFG-BlockAVDDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDUSBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365DriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365USBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MA.L2-3.7.5		Nonlocal Maintenance
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

Procedure Summary

[a]	The System Deployer configures the system such that multifactor authentication is required for nonlocal maintenance according to the System Baseline Standard.
[b]	The System Deployer configures the system such that nonlocal maintenance sessions are terminated when maintenance is complete according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.7.5[a]	Implemented

Assessment Objective

Multifactor authentication is used to establish nonlocal maintenance sessions via external network connections

Program Procedure

The System Deployer configures the system such that multifactor authentication is required for nonlocal maintenance according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure Multifactor Authentication Methods in the Entra Portal
- Configure Role-Based Access Control (RBAC) groups with Microsoft Entra Privileged Identity Management (PIM) eligible role assignments. Role activations require a justification statement by default.

Qualys

- AVD Patch Inventory is configured using Azure Runbooks to enable Qualys agent scanning

Win 10/11 AVD

- Configure CAP-RequireMFAEachSigninToAVD-EID to require users to provide authentication each sign-in to the AVD.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.

Configuration Evidence

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

CAP-RequireMFAEachSigninToAVD-EID
- Entra Admin Portal > Security > Conditional Access

Entra Authentication Methods Screenshot
- Entra Portal > Protection > Authentication Methods > Manage > Policies

Qualys Agent Dashboard
- Qualys > Agent Dashboard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Roles Defined in Entra PIM

- Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Roles > All Roles
  or
  Microsoft Entra Admin Center > Identity Governance > Privileged Identity Management > Manage > Groups > All Groups

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.7.5[b]	Implemented

Assessment Objective

Nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete

Program Procedure

The System Deployer configures the system such that nonlocal maintenance sessions are terminated when maintenance is complete according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Idle Session Timeout in the M365 admin center to sign users automatically out of Microsoft 365 web apps after sixty (60) minutes.
- Set the Directory Level Idle Timeout in Azure to sixty (60) minutes.

Qualys

- AVD Patch Inventory is configured using Azure Runbooks to enable Qualys agent scanning

Win 10/11 AVD

- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes

Win 10/11 Win365

- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes

Configuration Evidence

CFG-DisconnectIdleRemoteSessions-INT
- Go to Intune Admin Center → Devices → Configuration

CFG-RemoveIdleDisconnectedSessions-INT
- Go to Intune Admin Center → Devices → Configuration

Directory Level Idle Timeout
- Azure > Top Right Settings Cog > Signing Out + Notifications > Enable Directory Level Timeout

Idle Session Timeout
- Microsoft Admin Center (portal.office365.us/adminportal) > Settings > Org Settings > Security and Privacy > Idle Session Timeout

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Qualys Agent Dashboard

- Qualys > Agent Dashboard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MA.L2-3.7.6		Maintenance Personnel
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Supervise the maintenance activities of maintenance personnel without required access authorization.

Procedure Summary

[a]	The System Administrator supervises external maintenance personnel during maintenance according to the Maintenance Personnel Section in the 3.7 Maintenance Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.7.6[a]	Implemented

Assessment Objective

Maintenance personnel without required access authorization are supervised during maintenance activities

Program Procedure

The System Administrator supervises external maintenance personnel during maintenance according to the Maintenance Personnel Section in the 3.7 Maintenance Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	System Administrator	Govern Team System Administrator System Security Analyst

Process Summary

- The Govern Team documents external maintenance personnel without required access authorization are supervised during maintenance activities in the Maintenance Personnel Section in the 3.7 Maintenance Policy.
- The System Administrator receives a Maintenance Case for granting access to external maintenance personnel.
- The System Administrator creates a temporary account for external maintenance personnel.
- The System Security Analyst monitors logs during maintenance by external maintenance personnel using the Security Monitoring Output Log.
- The System Administrator revokes the temporary account for external maintenance personnel after maintenance is complete.
- The System Administrator logs the revocation of the account in the Identity and Access Management Case.

Process Evidence

Identity and Access Management Case
- support.ardalyst.com

Maintenance Case
- support.ardalyst.com

Maintenance Personnel Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.7 Maintenance Policy

Security Monitoring Output Log
- SharePoint > Govern Docs > Artifacts > Security Monitoring Output Log

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Practice Code		Practice Name
MP.L2-3.8.1		Media Protection
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

Procedure Summary

[a]	The Govern Team documents that non-digital (e.g. paper) media containing CUI is not permitted, and documents in the Media Protection Section in the 3.8 Media Protection Policy.
[b]	The Govern Team documents that digital media containing CUI is not permitted, and documents in the Media Protection Section in the 3.8 Media Protection Policy.
[c]	The Govern Team documents that non-digital (e.g. paper) media containing CUI is not permitted, and documents in the Media Protection Section in the 3.8 Media Protection Policy.
[d]	The Govern Team documents that digital media containing CUI is not permitted, and documents in the Media Protection Section in the 3.8 Media Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.1[a]	Implemented

Assessment Objective

Paper media containing CUI is physically controlled

Program Procedure

The Govern Team documents that non-digital (e.g. paper) media containing CUI is not permitted, and documents in the Media Protection Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director decides that the organization does not permit the use of non-digital system media containing CUI.
- The Govern Team documents what types of CUI are permitted and not permitted in the Media Protection Section in the 3.8 Media Protection Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Media Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.1[b]	Implemented

Assessment Objective
Digital media containing CUI is physically controlled

Program Procedure
The Govern Team documents that digital media containing CUI is not permitted, and documents in the Media Protection Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director decides that the organization does not permit the use of digital system media containing CUI.
- The Govern Team documents what types of CUI are permitted and not permitted in the Media Protection Section in the 3.8 Media Protection Policy.

Process Evidence

Media Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.1[c]	Implemented

Assessment Objective

Paper media containing CUI is securely stored

Program Procedure

The Govern Team documents that non-digital (e.g. paper) media containing CUI is not permitted, and documents in the Media Protection Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director decides that the organization does not permit the use of non-digital system media containing CUI.
- The Govern Team documents what types of CUI are permitted and not permitted in the Media Protection Section in the 3.8 Media Protection Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Media Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.1[d]	Implemented

Assessment Objective

Digital media containing CUI is securely stored

Program Procedure

The Govern Team documents that digital media containing CUI is not permitted, and documents in the Media Protection Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director decides that the organization does not permit the use of digital system media containing CUI.
- The Govern Team documents what types of CUI are permitted and not permitted in the Media Protection Section in the 3.8 Media Protection Policy.

Process Evidence

Media Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MP.L2-3.8.2		Media Access
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Limit access to CUI on system media to authorized users.

Procedure Summary

[a]	The Govern Team documents that no physical media containing CUI is permitted in the environment in the Media Access Section in the 3.8 Media Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.2[a]	Implemented

Assessment Objective

Access to CUI on system media is limited to authorized users

Program Procedure

The Govern Team documents that no physical media containing CUI is permitted in the environment in the Media Access Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director decides that the organization does not permit the use of non-digital system media containing CUI.
- The Cybersecurity Program Director decides that the organization does not permit the use of digital system media containing CUI.
- The Govern Team documents that no physical media containing CUI is present in the environment in the Media Access Section in the 3.8 Media Protection Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Media Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

Media Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MP.L2-3.8.3		Media Disposal
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Sanitize or destroy system media containing CUI before disposal or release for reuse.

Procedure Summary

[a]	The Cloud Service Provider sanitizes or destroys media before disposal according to the Media Disposal Section in the 3.8 Media Protection Policy.
[b]	The Cloud Service Provider sanitizes media before it is reused according to the Media Disposal Section in the 3.8 Media Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.3[a]	Implemented

Assessment Objective

System media containing CUI is sanitized or destroyed before disposal

Program Procedure

The Cloud Service Provider sanitizes or destroys media before disposal according to the Media Disposal Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Cloud Service Provider	Cloud Service Provider

Configuration Summary

M365 GCC-H

- Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware by default.

Win 10/11 AVD

- Azure Disk Encryption with FIPS 140-2 validated modules, followed by cryptographic key purge, satisfies the NIST SP 800-88 'Purge' method for sanitization prior to disposal or reuse by default

Win 10/11 Win365

- Azure Disk Encryption with FIPS 140-2 validated modules, followed by cryptographic key purge, satisfies the NIST SP 800-88 'Purge' method for sanitization prior to disposal or reuse by default

Configuration Evidence

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.3[b]	Implemented

Assessment Objective

System media containing CUI is sanitized before it is released for reuse

Program Procedure

The Cloud Service Provider sanitizes media before it is reused according to the Media Disposal Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Cloud Service Provider	Cloud Service Provider

Configuration Summary

M365 GCC-H

- Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware by default.

Win 10/11 AVD

- Azure Disk Encryption with FIPS 140-2 validated modules, followed by cryptographic key purge, satisfies the NIST SP 800-88 'Purge' method for sanitization prior to disposal or reuse by default

Win 10/11 Win365

- Azure Disk Encryption with FIPS 140-2 validated modules, followed by cryptographic key purge, satisfies the NIST SP 800-88 'Purge' method for sanitization prior to disposal or reuse by default

Configuration Evidence

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MP.L2-3.8.4		Media Markings
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Mark media with necessary CUI markings and distribution limitations.

Procedure Summary

[a]	The Authorized User marks media with applicable CUI markings according to the Media Marking Section in the 3.8 Media Protection Policy.
[b]	The Authorized User marks media with distribution limitations according to the Media Marking Section in the 3.8 Media Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.4[a]	Implemented

Assessment Objective

Media containing CUI is marked with applicable CUI markings

Program Procedure

The Authorized User marks media with applicable CUI markings according to the Media Marking Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Authorized User	Authorized User

Configuration Summary

M365 GCC-H

- Digital CUI documents are marked according to federal guidelines

Configuration Evidence

NARA CUI Marking Handbook

- https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.4[b]	Implemented

Assessment Objective

Media containing CUI is marked with distribution limitations

Program Procedure

The Authorized User marks media with distribution limitations according to the Media Marking Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Authorized User	Authorized User

Configuration Summary

M365 GCC-H

- Digital CUI documents are marked according to federal guidelines

Configuration Evidence

NARA CUI Marking Handbook

- https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MP.L2-3.8.5		Media Accountability
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

Procedure Summary

[a]	The Govern Team documents that no physical media containing CUI is permitted in the environment in the Media Accountability Section in the 3.8 Media Protection Policy.
[b]	The Govern Team documents that no physical media containing CUI is permitted in the environment in the Media Accountability Section in the 3.8 Media Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.5[a]	Implemented

Assessment Objective

Access to media containing CUI is controlled

Program Procedure

The Govern Team documents that no physical media containing CUI is permitted in the environment in the Media Accountability Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director decides that the organization does not permit the use of non-digital system media containing CUI.
- The Cybersecurity Program Director decides that the organization does not permit the use of digital system media containing CUI.
- The Govern Team documents that no physical media containing CUI is permitted in the environment in the Media Accountability Section in the 3.8 Media Protection Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Media Accountability Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

Media Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.5[b]	Implemented

Assessment Objective

Accountability for media containing CUI is maintained during transport outside of controlled areas

Program Procedure

The Govern Team documents that no physical media containing CUI is permitted in the environment in the Media Accountability Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director decides that the organization does not permit the use of non-digital system media containing CUI.
- The Cybersecurity Program Director decides that the organization does not permit the use of digital system media containing CUI.
- The Govern Team documents that no physical media containing CUI is permitted in the environment in the Media Accountability Section in the 3.8 Media Protection Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Media Accountability Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

Media Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MP.L2-3.8.6		Portable Storage Encryption
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Procedure Summary

[a]	The Govern Team documents that no portable storage devices containing CUI are permitted in the environment in the Portable Storage Encryption Section in the 3.8 Media Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.6[a]	Implemented

Assessment Objective

The confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards

Program Procedure

The Govern Team documents that no portable storage devices containing CUI are permitted in the environment in the Portable Storage Encryption Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines that portable storage devices containing CUI are not permitted in the enclave.
- The Govern Team documents that portable storage devices containing CUI are not permitted in the enclave in the Portable Storage Encryption Section in the 3.8 Media Protection Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Portable Storage Encryption Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MP.L2-3.8.7		Removeable Media
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Control the use of removable media on system components.

Procedure Summary

[a]	The Govern Team documents that portable storage devices are not permitted in the Removable Media Section in the 3.8 Media Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.7[a]	Implemented

Assessment Objective

The use of removable media on system components is controlled

Program Procedure

The Govern Team documents that portable storage devices are not permitted in the Removable Media Section in the 3.8 Media Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Govern Team	Govern Team

Configuration Summary

Win 10/11 AVD

- Configure CFG-BlockAVDDriveRedirection-INT to block drive redirection to client endpoints from AVD sessions.
- Configure CFG-BlockAVDUSBDriveRedirection-INT to block AVD drive redirection to client endpoints from AVD sessions

Win 10/11 Win365

- Configure CFG-BlockW365DriveRedirection-INT to block drive redirection to client endpoints from W365 sessions
- Configure CFG-BlockW365USBDriveRedirection-INT to block USB drive redirection to client endpoints from W365 sessions

Configuration Evidence

CFG-BlockAVDDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockAVDUSBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365DriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-BlockW365USBDriveRedirection-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MP.L2-3.8.8		Shared Media
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Prohibit the use of portable storage devices when such devices have no identifiable owner.

Procedure Summary

[a]	The Govern Team documents that portable storage devices are not permitted in the enclave.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.8[a]	Implemented

Assessment Objective

The use of portable storage devices is prohibited when such devices have no identifiable owner

Program Procedure

The Govern Team documents that portable storage devices are not permitted in the enclave.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines that portable storage devices are not permitted.
- The Govern Team documents that portable storage devices are not permitted in the Shared Media Section in the 3.8 Media Protection Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Shared Media Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
MP.L2-3.8.9		Protect Backups
SPRS Value	**SPRS Score**	**Practice Status**
1	1	Implemented

Practice Statement

Protect the confidentiality of backup CUI at storage locations.

Procedure Summary

[a]	The Govern Team documents that no physical backups containing CUI are permitted.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.8.9[a]	Implemented

Assessment Objective

The confidentiality of backup CUI is protected at storage locations

Program Procedure

The Govern Team documents that no physical backups containing CUI are permitted.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents that no physical backups are permitted in the Protecting Backups Section in the 3.8 Media Protection Policy.

Process Evidence

Protecting Backups Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.8 Media Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
PS.L2-3.9.1		Screen Individuals
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Screen individuals prior to authorizing access to organizational systems containing CUI.

Procedure Summary

[a]	The Human Resources Team evaluates personnel for trustworthiness and suitability for accessing sensitive information.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.9.1[a]	Implemented

Assessment Objective

Individuals are screened prior to authorizing access to organizational systems containing CUI

Program Procedure

The Human Resources Team evaluates personnel for trustworthiness and suitability for accessing sensitive information.

Procedure Type	Responsible Role	Supporting Roles
Process	Human Resources Team	Human Resources Team

Process Summary

- The Human Resources Team conducts appropriate background checks based on personnels' assigned roles.
- The Human Resources Team stores the results of the background check.

Process Evidence

Background Check
- SharePoint > Govern Documents > Artifacts > Background Check

Onboarding / Offboarding Checklist
- SharePoint > Govern Docs > Artifacts > Onboarding / Offboarding Checklist Folder

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
PS.L2-3.9.2		Personnel Actions
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Procedure Summary

[a]	The Cybersecurity Program Director establishes policy and process for terminating system access and credentials during personnel actions.
[b]	The Technical Lead ensures system access and credentials are terminated or modified following personnel actions.
[c]	The Human Resources Team ensures the system is protected during and after personnel transfer actions.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.9.2[a]	Implemented

Assessment Objective

A policy and/or process for terminating system access and any credentials coincident with personnel actions is established

Program Procedure

The Cybersecurity Program Director establishes policy and process for terminating system access and credentials during personnel actions.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director designates a policy and process for managing access to the enclave during personnel reassignment and termination.
- The Govern Team documents the Personnel Actions Section in the 3.9 Personnel Security Policy.

Process Evidence

Personnel Actions Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.9 Personnel Security Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.9.2[b]	Implemented

Assessment Objective

System access and credentials are terminated consistent with personnel actions such as termination or transfer

Program Procedure

The Technical Lead ensures system access and credentials are terminated or modified following personnel actions.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Human Resources Team Operate Team System Administrator Technical Lead

Process Summary

- For planned terminations, Human Resources Team notifies the Technical Lead of a termination.
- Technical Lead notifies the Operate Team of the planned termination by opening an Identity and Access Management Case.
- Operate Team references the User, Process, and Asset Inventory to determine what systems the user can access.
- System Administrator disables account(s) on the planned termination date.
- System Administrator updates the User, Process, and Asset Inventory with the revoked system access and closes the case.
- Human Resources Team references the User, Process, and Asset Inventory to determine what Assets the employee must return.
- Operate Team notifies System Administrators of the planned termination by routing the Identity and Access Management Case.
- Human Resources Team facilitates the return of all company Assets, including IT equipment, badges, access cards and/or keys.
- For unplanned terminations, Human Resources Team notifies the Technical Lead of an unplanned termination.
- Technical Lead references the User, Process, and Asset Inventory to determine what systems the user can access.
- Technical Lead disables the employee's account(s) immediately.
- Technical Lead updates the User, Process, and Asset Inventory with the revoked system access.
- Technical Lead notifies the Operate Team of the unplanned termination by opening an Identity and Access Management Case.
- Operate Team reviews the unplanned termination actions to ensure all appropriate actions have been properly conducted and updates the User, Process, and Asset Inventory if needed.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- Human Resources Team conducts an exit interview, which includes a reminder that the employee has an obligation not to discuss or disclose CUI, even after employment ends.

Process Evidence

Identity and Access Management Case
- support.ardalyst.com

Onboarding / Offboarding Checklist
- SharePoint > Govern Docs > Artifacts > Onboarding / Offboarding Checklist Folder

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Assessment Objective Identifier	Assessment Objective Status
3.9.2[c]	Implemented

Assessment Objective

The system is protected during and after personnel transfer actions

Program Procedure

The Human Resources Team ensures the system is protected during and after personnel transfer actions.

Procedure Type	Responsible Role	Supporting Roles
Process	Human Resources Team	Human Resources Team Operate Team System Administrator Technical Lead

Process Summary

- For personnel transfers, Human Resources Team notifies the Technical Lead of the personnel transfer and the employee's new roles.
- Technical Lead assigns an updated Identity and RBAC based on their new role, and creates an Identity and Access Management Case to complete Identity Configuration.
- Operate Team updates the User, Process, and Asset Inventory with new Identity and RBAC information.
- Operate Team notifies the System Administrator(s) of updated Identity and RBAC information by opening Identity and Access Management Cases.
- System Administrator updates the User Identity with correct RBAC membership and closes the Identity and Access Management Case.

Process Evidence

Identity and Access Management Case
- support.ardalyst.com

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
PE.L2-3.10.1		Limit Physical Access
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

Procedure Summary

[a]	The Govern Team documents that no physical spaces containing CUI are in scope in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.
[b]	The Govern Team documents that no physical spaces containing CUI are in scope in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.
[c]	The Govern Team documents that no physical spaces containing CUI are in scope in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.
[d]	The Govern Team documents that no physical spaces containing CUI are in scope in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.1[a]	Implemented

Assessment Objective

Authorized individuals allowed physical access are identified

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that there are no physical spaces containing CUI in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Limiting Physical Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.1[b]	Implemented

Assessment Objective

Physical access to organizational systems is limited to authorized individuals

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that there are no physical spaces containing CUI in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Limiting Physical Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.1[c]	Implemented

Assessment Objective

Physical access to equipment is limited to authorized individuals

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that there are no physical spaces containing CUI in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Limiting Physical Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.1[d]	Implemented

Assessment Objective

Physical access to operating environments is limited to authorized individuals

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that there are no physical spaces containing CUI in the Limiting Physical Access Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Limiting Physical Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
PE.L2-3.10.2		Monitor Facility
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Protect and monitor the physical facility and support infrastructure for organizational systems.

Procedure Summary

[a]	The Govern Team documents that no physical spaces containing CUI are in scope in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.
[b]	The Govern Team documents that no physical spaces containing CUI are in scope in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.
[c]	The Govern Team documents that no physical spaces containing CUI are in scope in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.
[d]	The Govern Team documents that no physical spaces containing CUI are in scope in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.2[a]	Implemented

Assessment Objective

The physical facility where organizational systems reside is protected

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that no physical spaces containing CUI in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Monitoring the Facility Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.2[b]	Implemented

Assessment Objective

The support infrastructure for organizational systems is protected

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that no physical spaces containing CUI in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Monitoring the Facility Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.2[c]	Implemented

Assessment Objective

The physical facility where organizational systems reside is monitored

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that no physical spaces containing CUI in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Monitoring the Facility Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.2[d]	Implemented

Assessment Objective

The support infrastructure for organizational systems is monitored

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that no physical spaces containing CUI in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Monitoring the Facility Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
PE.L2-3.10.3		Escort Visitors
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Escort visitors and monitor visitor activity.

Procedure Summary

[a]	The Govern Team documents that no physical spaces containing CUI are in scope in the Escorting Visitors Section in the 3.10 Physical Protection Policy.
[b]	The Govern Team documents that no physical spaces containing CUI are in scope in the Escorting Visitors Section in the 3.10 Physical Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.3[a]	Implemented

Assessment Objective

Visitors are escorted

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Escorting Visitors Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that no physical spaces containing CUI are in scope in the Escorting Visitors Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Escorting Visitors Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.3[b]	Implemented

Assessment Objective

Visitor activity is monitored

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Escorting Visitors Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that no physical spaces containing CUI are in scope in the Escorting Visitors Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Escorting Visitors Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
PE.L2-3.10.4		Physical Access Logs
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Maintain audit logs of physical access.

Procedure Summary

[a]	The Govern Team documents that no physical spaces containing CUI are in scope in the Physical Access Logs Section in the 3.10 Physical Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.4[a]	Implemented

Assessment Objective

Audit logs of physical access are maintained

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Physical Access Logs Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that there are no physical spaces containing CUI in the Physical Access Logs Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Physical Access Logs Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
PE.L2-3.10.5		Manage Physical Access
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Control and manage physical access devices.

Procedure Summary

[a]	The Govern Team documents that no physical spaces containing CUI are in scope in the Managing Physical Access Section in the 3.10 Physical Protection Policy.
[b]	The Govern Team documents that no physical spaces containing CUI are in scope in the Managing Physical Access Section in the 3.10 Physical Protection Policy.
[c]	The Govern Team documents that no physical spaces containing CUI are in scope in the Managing Physical Access Section in the 3.10 Physical Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.5[a]	Implemented

Assessment Objective

Physical access devices are identified

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Managing Physical Access Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that no physical spaces containing CUI are in scope in the Managing Physical Access Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Managing Physical Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.5[b]	Implemented

Assessment Objective

Physical access devices are controlled

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Managing Physical Access Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that no physical spaces containing CUI are in scope in the Managing Physical Access Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Managing Physical Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.5[c]	Implemented

Assessment Objective

Physical access devices are managed

Program Procedure

The Govern Team documents that no physical spaces containing CUI are in scope in the Managing Physical Access Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines if there are physical spaces containing CUI.
- The Govern Team documents that no physical spaces containing CUI are in scope in the Managing Physical Access Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Managing Physical Access Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
PE.L2-3.10.6		Alternative Work Sites
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Enforce safeguarding measures for CUI at alternate work sites.

Procedure Summary

[a]	The Govern Team documents that alternate worksites are not allowed in the Alternative Work Sites Section in the 3.10 Physical Protection Policy.
[b]	The Govern Team documents that alternate worksites are not permitted in the Alternative Work Sites Section in the 3.10 Physical Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.6[a]	Implemented

Assessment Objective

Safeguarding measures for CUI are defined for alternate work sites

Program Procedure

The Govern Team documents that alternate worksites are not allowed in the Alternative Work Sites Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines that there are no alternative worksites.
- The Govern Team documents that no alternative worksites are permitted in the Alternative Work Sites Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Alternative Work Sites Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.10.6[b]	Implemented

Assessment Objective

Safeguarding measures for CUI are enforced for alternate work sites

Program Procedure

The Govern Team documents that alternate worksites are not permitted in the Alternative Work Sites Section in the 3.10 Physical Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines that there are no alternative worksites.
- The Govern Team documents that no alternative worksites are permitted in the Alternative Work Sites Section in the 3.10 Physical Protection Policy.
- The Govern Team documents that third party physical datacenter security is managed by the external service provider in the Monitoring the Facility Section in the 3.10 Physical Protection Policy.

Process Evidence

Alternative Work Sites Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.10 Physical Protection Policy

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
RA.L2-3.11.1		Risk Assessments
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Procedure Summary

[a]	The Govern Team defines frequency with which the organization performs Risk Assessments and documents in the Risk Assessments Section in the 3.11 Risk Assessment Policy.
[b]	The Govern Team leads performance of the risk assessment in accordance with the Risk Assessments Section in the 3.11 Risk Assessment Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.11.1[a]	Implemented

Assessment Objective

The frequency to assess risk to organizational operations, organizational assets, and individuals is defined

Program Procedure

The Govern Team defines frequency with which the organization performs Risk Assessments and documents in the Risk Assessments Section in the 3.11 Risk Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team defines frequency to assess organizational risk.
- The Govern Team documents the frequency for risk assessments in the Risk Assessments Section in the 3.11 Risk Assessment Policy.

Process Evidence

Risk Assessments Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.11 Risk Assessment Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.11.1[b]	Implemented

Assessment Objective

Risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency

Program Procedure

The Govern Team leads performance of the risk assessment in accordance with the Risk Assessments Section in the 3.11 Risk Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Govern Team notifies the Cybersecurity Program Director of the need to conduct a risk assessment in accordance with the Risk Assessments Section in the 3.11 Risk Assessment Policy.
- The Govern Team conducts a risk assessment based on the completed Scope Enclave Diagram and CUI Flow Diagram.
- The Cybersecurity Program Director reviews the completed Risk Assessment.
- The Cybersecurity Program Director accepts the Risk Assessment.

Process Evidence

Risk Assessment
- SharePoint > Govern Docs > Artifacts > Risk Assessment

Risk Assessments Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.11 Risk Assessment Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
RA.L2-3.11.2		Vulnerability Scan
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Procedure Summary

[a]	The Govern Team defines the vulnerability scan frequency in the Vulnerability Scanning Section in the 3.11 Risk Assessment Policy.
[b]	The System Security Analyst performs vulnerability scans on organizational systems with the defined frequency according to the System Baseline Standard.
[c]	The System Security Analyst performs vulnerability scans on applications with the defined frequency according to the System Baseline Standard.
[d]	The System Security Analyst conducts vulnerability scans on organizational systems when new vulnerabilities are identified according to the System Baseline Standard.
[e]	The System Security Analyst conducts vulnerability scans on applications when new vulnerabilities are identified according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.11.2[a]	Implemented

Assessment Objective

The frequency to scan for vulnerabilities in organizational systems and applications is defined

Program Procedure

The Govern Team defines the vulnerability scan frequency in the Vulnerability Scanning Section in the 3.11 Risk Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team Technical Lead

Process Summary

- The Technical Lead defines the frequency to scan for vulnerabilities in organizational systems and applications as no more than thirty (30) days.
- The Govern Team documents the vulnerability scan frequency in the Vulnerability Scanning Section in the 3.11 Risk Assessment Policy.

Process Evidence

Vulnerability Scanning Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.11 Risk Assessment Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.11.2[b]	Implemented

Assessment Objective

Vulnerability scans are performed on organizational systems with the defined frequency

Program Procedure

The System Security Analyst performs vulnerability scans on organizational systems with the defined frequency according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Qualys

- A Qualys Patch Management Agent is deployed to scan for, and automatically remediate vulnerabilities via patches made available by vendors.
- AVD Patch Inventory is configured using Azure Runbooks to enable Qualys agent scanning

Win 10/11 AVD

- Configure an Automation Account within Azure to start AVDs on Friday morning for patch cycle.
- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Win 10/11 Win365

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Configuration Evidence

Automation Account for Patch
- Azure portal > Automation Account

CFG-VulnerabilityScans-INT
- Microsoft Defender Portal > Endpoints > Configuration Management > Endpoint Security Policies

Qualys Agent Dashboard
- Qualys > Agent Dashboard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.11.2[c]	Implemented

Assessment Objective

Vulnerability scans are performed on applications with the defined frequency

Program Procedure

The System Security Analyst performs vulnerability scans on applications with the defined frequency according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Qualys

- A Qualys Patch Management Agent is deployed to scan for, and automatically remediate vulnerabilities via patches made available by vendors.
- AVD Patch Inventory is configured using Azure Runbooks to enable Qualys agent scanning

Win 10/11 AVD

- Configure an Automation Account within Azure to start AVDs on Friday morning for patch cycle.
- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Win 10/11 Win365

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Configuration Evidence

Automation Account for Patch
- Azure portal > Automation Account

CFG-VulnerabilityScans-INT
- Microsoft Defender Portal > Endpoints > Configuration Management > Endpoint Security Policies

Qualys Agent Dashboard
- Qualys > Agent Dashboard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.11.2[d]	Implemented

Assessment Objective

Vulnerability scans are performed on organizational systems when new vulnerabilities are identified

Program Procedure

The System Security Analyst conducts vulnerability scans on organizational systems when new vulnerabilities are identified according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Qualys

- A Qualys Patch Management Agent is deployed to scan for, and automatically remediate vulnerabilities via patches made available by vendors.

Win 10/11 AVD

- Configure an Automation Account within Azure to start AVDs on Friday morning for patch cycle.
- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Win 10/11 Win365

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Configuration Evidence

Automation Account for Patch
- Azure portal > Automation Account

CFG-VulnerabilityScans-INT
- Microsoft Defender Portal > Endpoints > Configuration Management > Endpoint Security Policies

Qualys Agent Dashboard
- Qualys > Agent Dashboard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.11.2[e]	Implemented

Assessment Objective

Vulnerability scans are performed on applications when new vulnerabilities are identified

Program Procedure

The System Security Analyst conducts vulnerability scans on applications when new vulnerabilities are identified according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Qualys

- A Qualys Patch Management Agent is deployed to scan for, and automatically remediate vulnerabilities via patches made available by vendors.

Win 10/11 AVD

- Configure an Automation Account within Azure to start AVDs on Friday morning for patch cycle.
- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Win 10/11 Win365

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Configuration Evidence

Automation Account for Patch
- Azure portal > Automation Account

CFG-VulnerabilityScans-INT
- Microsoft Defender Portal > Endpoints > Configuration Management > Endpoint Security Policies

Qualys Agent Dashboard
- Qualys > Agent Dashboard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
RA.L2-3.11.3		Vulnerability Remediation
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Remediate vulnerabilities in accordance with risk assessments.

Procedure Summary

[a] The System Security Analyst identifies vulnerabilities.

[b] The System Maintainer remediates identified vulnerabilities.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.11.3[a]	Implemented

Assessment Objective

Vulnerabilities are identified

Program Procedure

The System Security Analyst identifies vulnerabilities.

Procedure Type	Responsible Role	Supporting Roles
Process	System Security Analyst	Govern Team System Security Analyst

Process Summary

- The Govern Team documents that critical vulnerabilities must be remediated within 30 days, while high vulnerabilities must be addressed within 60 days, medium risk vulnerabilities within 90, and low within 180 in the Vulnerability Remediation Section in the 3.11 Risk Assessment Policy.
- The System Security Analyst reviews the patch management system for alerts.
- The System Security Analyst reviews Threat Analytics in the SIEM for vulnerabilities.
- The System Security Analyst opens a Maintenance Case for each Critical and High Vulnerability found.
- The System Security Analyst assigns the Maintenance Case to the System Maintainer.

Process Evidence

Maintenance Case
- support.ardalyst.com

Security Monitoring Output Log
- SharePoint > Govern Docs > Artifacts > Security Monitoring Output Log

Vulnerability Remediation Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.11 Risk Assessment Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Assessment Objective Identifier	Assessment Objective Status
3.11.3[b]	Implemented

Assessment Objective

Vulnerabilities are remediated in accordance with risk assessments

Program Procedure

The System Maintainer remediates identified vulnerabilities.

Procedure Type	Responsible Role	Supporting Roles
Process	System Maintainer	System Maintainer

Process Summary

- The System Maintainer patches the vulnerability if there is a patch available.
- The System Maintainer escalates the Maintenance Case to the Escalation Support Team if there is not a patch available.
- The System Maintainer updates and closes the case in CRM.

Process Evidence

Maintenance Case
- support.ardalyst.com

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CA.L2-3.12.1		Security Control Assessment
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Procedure Summary

[a]	The Govern Team defines that security control assessments will be conducted at least every one (1) year according to the Security Control Assessment Section in the 3.12 Security Assessment Policy.
[b]	The Defend Team assesses security controls at least every one (1) year according to the Security Control Assessment Section in the 3.12 Security Assessment Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.1[a]	Implemented

Assessment Objective

The frequency of security control assessments is defined

Program Procedure

The Govern Team defines that security control assessments will be conducted at least every one (1) year according to the Security Control Assessment Section in the 3.12 Security Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team defines the frequency of security control assessments as at least every one (1) year.
- The Govern Team documents the frequency of security control assessments in the Security Control Assessment Section in the 3.12 Security Assessment Policy.

Process Evidence

Security Control Assessment Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.12 Security Assessment Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.1[b]	Implemented

Assessment Objective

Security controls are assessed with the defined frequency to determine if the controls are effective in their application

Program Procedure

The Defend Team assesses security controls at least every one (1) year according to the Security Control Assessment Section in the 3.12 Security Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Defend Team	Defend Team

Process Summary

- The Defend Team assesses security controls at least every one (1) year according to the Security Control Assessment Section in the 3.12 Security Assessment Policy.
- The Defend Team documents the output of the security control assessment in the Security Control Assessment Report.
- The Defend Team proposes new controls; updates to existing controls; and remediation plans; and documents them in the Security Control Assessment Report.
- The Defend Team documents newly identified risks in Security Control Assessment Report.

Process Evidence

Security Control Assessment Report
- SharePoint > Govern Docs > Artifacts > Security Control Assessment Report

Security Control Assessment Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.12 Security Assessment Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CA.L2-3.12.2		Operational Plan of Action
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Procedure Summary

[a]	The Govern Team identifies deficiencies and vulnerabilities to be addressed and documents them in the Operational Plan of Action according to the Plan of Action Section in the 3.12 Security Assessment Policy.
[b]	The Govern Team ensures the Operational Plan of Action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.
[c]	The Govern Team ensures that the Operational Plan of Action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.2[a]	Implemented

Assessment Objective

Deficiencies and vulnerabilities to be addressed by the plan of action are identified

Program Procedure

The Govern Team identifies deficiencies and vulnerabilities to be addressed and documents them in the Operational Plan of Action according to the Plan of Action Section in the 3.12 Security Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents the Plan of Action Section in the 3.12 Security Assessment Policy.
- The Govern Team reviews the Incident Response Plan and documents deficiencies and vulnerabilities in the Operational Plan of Action.
- The Govern Team reviews the News Review Log and documents deficiencies and vulnerabilities in the Operational Plan of Action.
- The Govern Team reviews the Publication Review Log and documents deficiencies and vulnerabilities in the Operational Plan of Action.
- The Govern Team reviews the Risk Assessment and documents deficiencies and vulnerabilities in the Operational Plan of Action.
- The Govern Team reviews the Security Control Assessment Report and documents deficiencies and vulnerabilities in the Operational Plan of Action.
- The Govern Team reviews the Security Impact Analysis and documents deficiencies and vulnerabilities in the Operational Plan of Action.
- The Govern Team reviews the Security Monitoring Output Log and documents deficiencies and vulnerabilities in the Operational Plan of Action.

Process Evidence

Operational Plan of Action
- SharePoint > Govern Docs > Artifacts > Operational Plan of Action

Plan of Action Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.12 Security Assessment Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.2[b]	Implemented

Assessment Objective

A plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities

Program Procedure

The Govern Team ensures the Operational Plan of Action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team System Designer Technical Lead

Process Summary

- The System Designer develops approaches to correct identified deficiencies.
- The System Designer develops estimates for time and resources to implement the approaches to correct identified deficiencies.
- The Technical Lead approves the estimates in the Operational Plan of Action.
- The Govern Team develops a plan of action for implementing the deficiencies based on the estimates and documents in the Operational Plan of Action.

Process Evidence

Operational Plan of Action
- SharePoint > Govern Docs > Artifacts > Operational Plan of Action

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.2[c]	Implemented

Assessment Objective

The plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities

Program Procedure

The Govern Team ensures that the Operational Plan of Action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team System Deployer System Designer System Security Analyst

Process Summary

- The Govern Team directs the System Designers to implement corrections according to the schedule in the Operational Plan of Action.
- The System Designer develops the configurations to correct identified deficiencies.
- The System Designer documents the configurations to correct identified deficiencies in the System Baseline Standard.
- The System Deployer configures the system such that identified deficiencies are corrected according to the System Baseline Standard.
- The System Security Analyst ensures that the configurations are deployed and functioning as desired.
- The Govern Team tracks the completion of implementations in the Operational Plan of Action.

Process Evidence

Operational Plan of Action
- SharePoint > Govern Docs > Artifacts > Operational Plan of Action

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
CA.L2-3.12.3		Security Control Monitoring
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Procedure Summary

[a]	The Defend Team monitors security controls to ensure their continued effectiveness according to the Security Control Monitoring Section in the 3.12 Security Assessment Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.3[a]	Implemented

Assessment Objective

Security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls

Program Procedure

The Defend Team monitors security controls to ensure their continued effectiveness according to the Security Control Monitoring Section in the 3.12 Security Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Defend Team	Defend Team Govern Team

Process Summary

- The Govern Team documents the monitoring of security controls according to the Security Control Monitoring Section in the 3.12 Security Assessment Policy.
- The Defend Team identifies security controls to be continuously monitored and documents in the Security Control Monitoring Plan.
- The Defend Team identifies the timeframe for continuous monitoring activities and documents in the Security Control Monitoring Plan.
- The Defend Team performs continuous monitoring according to the Security Control Monitoring Plan and documents in the Tesseract Protection Report.
- The Defend Team opens Event Investigation Cases for investigation and remediation.
- The Defend Team provides the Tesseract Protection Report to the Cybersecurity Program Director, the Technical Lead, and the Govern Team.

Process Evidence

Event Investigation Case
- support.ardalyst.com

Security Control Monitoring Plan
- SharePoint > Govern Docs > Artifacts > Security Control Monitoring Plan

Security Control Monitoring Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.12 Security Assessment Policy

Tesseract Protection Report
- SharePoint > Govern Docs > Artifacts > Tesseract Protection Report

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Practice Code		Practice Name
CA.L2-3.12.4		System Security Plan
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Procedure Summary

[a]	The Govern Team develops a System Security Plan according to the System Security Plan Section in the 3.12 Security Assessment Policy.
[b]	The Govern Team documents the system boundary according to the Scope Enclave and CUI Flow Diagram in the System Security Plan.
[c]	The Govern Team documents the system environment of operation according to the Scope Enclave and CUI Flow Diagram.
[d]	The Cybersecurity Program Director identifies the security requirements that are non-applicable in the System Security Plan.
[e]	The Govern Team describes the method of implementation for each security requirement and documents in the System Security Plan.
[f]	The Govern Team documents the relationship with or connection to other systems according to the Scope Enclave and CUI Flow Diagram.
[g]	The Govern Team defines the frequency to update the System Security Plan in the System Security Plan Section in the 3.12 Security Assessment Policy.
[h]	The Govern Team updates the System Security Plan according to the System Security Plan Section in the 3.12 Security Assessment Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.4[a]	Implemented

Assessment Objective

A system security plan is developed

Program Procedure

The Govern Team develops a System Security Plan according to the System Security Plan Section in the 3.12 Security Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Defend Team Govern Team Harden Team System Designer System Security Analyst Technical Lead

Process Summary

- The Govern Team documents the Plan of Actions and Milestones to record any Not Met controls.
- The Govern Team documents the Cybersecurity Policy Manual.
- The Govern Team documents the Tesseract Shared Responsibility Matrix.
- The Govern Team documents the requirements for the System Security Plan in the System Security Plan Section in the 3.12 Security Assessment Policy.
- The Govern Team develops the System Security Plan.
- The Technical Lead contributes content to the System Security Plan.
- The Cybersecurity Program Director contributes content to the System Security Plan.
- The Harden Team contributes content to the System Security Plan.
- The Defend Team contributes content to the System Security Plan.
- The System Designer contributes content to the System Security Plan.
- The System Security Analyst contributes content to the System Security Plan.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Plan of Actions and Milestones
- SharePoint > Govern Docs > Artifacts > Plan of Actions and Milestones

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

System Security Plan Section

- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.12 Security Assessment Policy

Tesseract Shared Responsibility Matrix

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.4[b]	Implemented

Assessment Objective

The system boundary is described and documented in the system security plan

Program Procedure

The Govern Team documents the system boundary according to the Scope Enclave and CUI Flow Diagram in the System Security Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team Technical Lead

Process Summary

- The Technical Lead identifies the external system boundary.
- The Technical Lead identifies the internal system boundary.
- The Govern Team illustrates the external system boundary in the Scope Enclave and CUI Flow Diagram.
- The Govern Team illustrates the internal system boundary in the Scope Enclave and CUI Flow Diagram.
- The Govern Team uploads the Scope Enclave and CUI Flow Diagram.

Process Evidence

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.4[c]	Implemented

Assessment Objective

The system environment of operation is described and documented in the system security plan

Program Procedure

The Govern Team documents the system environment of operation according to the Scope Enclave and CUI Flow Diagram.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Defend Team Govern Team Harden Team System Designer System Security Analyst Technical Lead

Process Summary

- The Govern Team describes the system environment of operation in the System Security Plan.
- The Technical Lead contributes content regarding the system environment of operation to the System Security Plan.
- The Cybersecurity Program Director contributes content regarding the system environment of operation to the System Security Plan.
- The Harden Team contributes content regarding the system environment of operation to the System Security Plan.
- The Defend Team contributes content regarding the system environment of operation to the System Security Plan.
- The System Designer contributes content regarding the system environment of operation to the System Security Plan.
- The System Security Analyst contributes content regarding the system environment of operation to the System Security Plan.

Process Evidence

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.4[d]	Implemented

Assessment Objective

The security requirements identified and approved by the designated authority as non-applicable are identified

Program Procedure

The Cybersecurity Program Director identifies the security requirements that are non-applicable in the System Security Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Cybersecurity Program Director	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director approves the assessment objectives that are not applicable.
- The Govern Team documents which assessment objectives are not applicable in the System Security Plan.

Process Evidence

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.4[e]	Implemented

Assessment Objective

The method of security requirement implementation is described and documented in the system security plan

Program Procedure

The Govern Team describes the method of implementation for each security requirement and documents in the System Security Plan.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Defend Team Govern Team Harden Team System Designer System Security Analyst Technical Lead

Process Summary

- The Govern Team describes the method of implementation for each security requirement and documents in the System Security Plan.
- The Technical Lead contributes content regarding the method of implementation for each security requirement and documents in the System Security Plan.
- The Cybersecurity Program Director contributes content regarding the method of implementation for each security requirement and documents in the System Security Plan.
- The Harden Team contributes technical architecture and system design content for each security requirement and documents in the System Security Plan.
- The Defend Team contributes logging, event management, reporting, and investigation content for each security requirement and documents in the System Security Plan.
- The System Designer contributes system design and configuration content for each security requirement and documents in the System Security Plan.
- The System Security Analyst contributes logging and event management content for each security requirement and documents in the System Security Plan.

Process Evidence

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.4[f]	Implemented

Assessment Objective

The relationship with or connection to other systems is described and documented in the system security plan

Program Procedure

The Govern Team documents the relationship with or connection to other systems according to the Scope Enclave and CUI Flow Diagram.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team Technical Lead

Process Summary

- The Technical Lead identifies how External Service Providers (ESPs) and Cloud Service Providers (CSPs) connect to organization owned systems.
- The Govern Team documents how External Service Providers (ESPs) and Cloud Service Providers (CSPs) connect to organization owned systems in the System Security Plan.

Process Evidence

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.4[g]	Implemented

Assessment Objective

The frequency to update the system security plan is defined

Program Procedure

The Govern Team defines the frequency to update the System Security Plan in the System Security Plan Section in the 3.12 Security Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team Technical Lead

Process Summary

- The Technical Lead defines the frequency to update the System Security Plan as annually.
- The Govern Team documents the frequency to update the System Security Plan as annually in the System Security Plan Section in the 3.12 Security Assessment Policy.
- The Govern Team updates the System Security Plan annually.

Process Evidence

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

System Security Plan Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.12 Security Assessment Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.12.4[h]	Implemented

Assessment Objective

System security plan is updated with the defined frequency

Program Procedure

The Govern Team updates the System Security Plan according to the System Security Plan Section in the 3.12 Security Assessment Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team Technical Lead

Process Summary

- The Cybersecurity Program Director signs the System Security Plan to indicate their acceptance of the plan and direct its adoption.
- The Technical Lead signs the System Security Plan to indicate their acceptance of the plan and direct its adoption.
- The Govern Team updates the System Security Plan annually.

Process Evidence

System Security Plan
- SharePoint > Govern Docs > Artifacts > System Security Plan

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.1		Boundary Protection
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

Procedure Summary

[a]	The Technical Lead defines the external system boundary in the Scope Enclave Diagram.
[b]	The Technical Lead defines the internal system boundary in the Scope Enclave Diagram.
[c]	The System Security Analyst monitors the external system boundary.
[d]	The System Security Analyst monitors the internal system boundary.
[e]	The System Deployer configures the system such that communications at the external system boundary are controlled according to the System Baseline Standard.
[f]	The System Deployer configures the system such that communications at the internal system boundary are controlled according to the System Baseline Standard.
[g]	The System Deployer configures the system such that communications at the external system boundary are protected according to the System Baseline Standard.
[h]	The System Deployer configures the system such that communications at the internal system boundary are protected according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.1[a]	Implemented

Assessment Objective

The external system boundary is defined

Program Procedure

The Technical Lead defines the external system boundary in the Scope Enclave Diagram.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team Technical Lead

Process Summary

- The Govern Team documents the requirements for boundary protection in the Boundary Protection Section in the 3.13 System and Communications Protection Policy.
- The Technical Lead identifies the external system boundary.
- The Govern Team illustrates the external system boundary in the Scope Enclave and CUI Flow Diagram.

Process Evidence

Boundary Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.1[b]	Implemented

Assessment Objective

Key internal system boundaries are defined

Program Procedure

The Technical Lead defines the internal system boundary in the Scope Enclave Diagram.

Procedure Type	Responsible Role	Supporting Roles
Process	Technical Lead	Govern Team Technical Lead

Process Summary

- The Govern Team documents the requirements for boundary protection in the Boundary Protection Section in the 3.13 System and Communications Protection Policy.
- The Technical Lead identifies the internal system boundary.
- The Govern Team illustrates the internal system boundary in the Scope Enclave and CUI Flow Diagram.

Process Evidence

Boundary Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.1[c]	Implemented

Assessment Objective

Communications are monitored at the external system boundary

Program Procedure

The System Security Analyst monitors the external system boundary.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- After connectors are set up, Defender XDR audits all cloud operations by default. Each audit log entry contains a user's immutable objectID that can be used to uniquely trace an individual system user to each action.
- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Configure Microsoft Entra ID data connector to send audit, sign in and non-interactive sign in logs to the Log Analytics Workspace.
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default
- Microsoft Sentinel provides audit reduction and report generation by default

Win 10/11 AVD

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Win 10/11 Win365

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Configuration Evidence

EDR-DeployDefenderConnector-INT

- Intune Portal > Endpoint Security > Endpoint Detection and Response

Microsoft CMMC Additional Controls Learn Article

- https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-additional-controls

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Microsoft Defender XDR to Sentinel Connector Learn Article

- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

Microsoft Entra ID Log Diagnostic Settings

- Entra ID > Monitoring > Diagnostic settings

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.1[d]	Implemented

Assessment Objective

Communications are monitored at key internal boundaries

Program Procedure

The System Security Analyst monitors the internal system boundary.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- After connectors are set up, Defender XDR audits all cloud operations by default. Each audit log entry contains a user's immutable objectID that can be used to uniquely trace an individual system user to each action.
- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Configure Microsoft Entra ID data connector to send audit, sign in and non-interactive sign in logs to the Log Analytics Workspace.
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default
- Microsoft Sentinel provides audit reduction and report generation by default

Win 10/11 AVD

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Win 10/11 Win365

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Configuration Evidence

EDR-DeployDefenderConnector-INT

- Intune Portal > Endpoint Security > Endpoint Detection and Response

Microsoft CMMC Additional Controls Learn Article

- https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-additional-controls

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Microsoft Defender XDR to Sentinel Connector Learn Article

- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

Microsoft Entra ID Log Diagnostic Settings

- Entra ID > Monitoring > Diagnostic settings

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.1[e]	Implemented

Assessment Objective

Communications are controlled at the external system boundary

Program Procedure

The System Deployer configures the system such that communications at the external system boundary are controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Microsoft Entra ID data connector to send audit, sign in and non-interactive sign in logs to the Log Analytics Workspace.
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Win 10/11 AVD

- Configure SCR-WinFirewallDenyByDefault-INT to deny inbound and outbound traffic by default.
- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Win 10/11 Win365

- Entra ID audit logs contain time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, and filenames where applicable by default.

Configuration Evidence

Microsoft Entra ID Log Diagnostic Settings
- Entra ID > Monitoring > Diagnostic settings

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

SCR-WinFirewallDenyByDefault-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.1[f]	Implemented

Assessment Objective

Communications are controlled at key internal boundaries

Program Procedure

The System Deployer configures the system such that communications at the internal system boundary are controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Microsoft Entra ID data connector to send audit, sign in and non-interactive sign in logs to the Log Analytics Workspace.
- Microsoft Sentinel provides audit reduction and report generation by default

Win 10/11 AVD

- Configure SCR-WinFirewallDenyByDefault-INT to deny inbound and outbound traffic by default.

Configuration Evidence

Microsoft Entra ID Log Diagnostic Settings
- Entra ID > Monitoring > Diagnostic settings

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

SCR-WinFirewallDenyByDefault-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.1[g]	Implemented

Assessment Objective

Communications are protected at the external system boundary

Program Procedure

The System Deployer configures the system such that communications at the external system boundary are protected according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-BlockUntrustedLocations-EID to block connections from untrusted locations
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 AVD

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Configure SCR-WinFirewallDenyByDefault-INT to deny inbound and outbound traffic by default.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Configuration Evidence

CAP-BlockUntrustedLocations-EID
- Entra Admin Portal > Security > Conditional Access

CAP-EnforceRRMFA-EID
- Entra Admin Portal > Security > Conditional Access

SCR-WinFirewallDenyByDefault-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

Technical Reference Details About Encryption Learn Article
- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.1[h]	Implemented

Assessment Objective

Communications are protected at key internal boundaries

Program Procedure

The System Deployer configures the system such that communications at the internal system boundary are protected according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 AVD

- Configure SCR-WinFirewallDenyByDefault-INT to deny inbound and outbound traffic by default.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Configuration Evidence

SCR-WinFirewallDenyByDefault-INT

- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

Technical Reference Details About Encryption Learn Article

- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.2		Security Engineering
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Procedure Summary

[a]	The Govern Team documents the architectural designs for information security in the Tesseract Security Architecture.
[b]	The Govern Team documents that the organization does not develop software in the Security Engineering Section in the 3.13 System and Communications Protection Policy.
[c]	The System Designer identifies systems engineering principles for information security in the Tesseract Security Architecture.
[d]	The System Deployer configures systems such that they follow the architectural designs according to the System Baseline Standard.
[e]	The Govern Team documents that the organization does not develop software in the Security Engineering Section in the 3.13 System and Communications Protection Policy.
[f]	The System Deployer configures systems such that they follow the systems engineering principles according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.2[a]	Implemented

Assessment Objective

Architectural designs that promote effective information security are identified

Program Procedure

The Govern Team documents the architectural designs for information security in the Tesseract Security Architecture.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team identifies the architectural designs for information security in the Tesseract Security Architecture.
- The Govern Team illustrates the architectural designs for information security in the Tesseract Security Architecture.

Process Evidence

Tesseract Security Architecture

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.2[b]	Implemented

Assessment Objective

Software development techniques that promote effective information security are identified

Program Procedure

The Govern Team documents that the organization does not develop software in the Security Engineering Section in the 3.13 System and Communications Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines that the organization does not develop software.
- The Govern Team documents that the organization does not develop software in the Security Engineering Section in the 3.13 System and Communications Protection Policy.

Process Evidence

Security Engineering Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.2[c]	Implemented

Assessment Objective

Systems engineering principles that promote effective information security are identified

Program Procedure

The System Designer identifies systems engineering principles for information security in the Tesseract Security Architecture.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	System Designer

Process Summary

- The System Designer identifies systems engineering principles for information security in the Tesseract Security Architecture.
- The System Designer documents systems engineering principles for information security in the Tesseract Security Architecture.

Process Evidence

Tesseract Security Architecture

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.2[d]	Implemented

Assessment Objective

Identified architectural designs that promote effective information security are employed

Program Procedure

The System Deployer configures systems such that they follow the architectural designs according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft Sentinel provides audit reduction and report generation by default
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 AVD

- Microsoft Antimalware automatically updates malicious code signatures by default.
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Microsoft Antimalware automatically updates malicious code signatures by default.
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Configuration Evidence

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Technical Reference Details About Encryption Learn Article

- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.2[e]	Implemented

Assessment Objective

Identified software development techniques that promote effective information security are employed

Program Procedure

The Govern Team documents that the organization does not develop software in the Security Engineering Section in the 3.13 System and Communications Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines that the organization does not develop software.
- The Govern Team documents that the organization does not develop software in the Security Engineering Section in the 3.13 System and Communications Protection Policy.

Process Evidence

Security Engineering Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.2[f]	Implemented

Assessment Objective

Identified systems engineering principles that promote effective information security are employed

Program Procedure

The System Deployer configures systems such that they follow the systems engineering principles according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.

Win 10/11 AVD

- Configure CFG-AVDWindowsUpdateForBusiness-INT to implement forced updates on AVD.
- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.
- Microsoft Antimalware automatically updates malicious code signatures by default.

Win 10/11 Win365

- Configure CFG-VulnerabilityScans-INT to scan for vulnerabilities on endpoints.
- Configure Windows Update Ring WUR-WindowsUpdateRing-INT to enforce Windows updates on managed endpoints
- Microsoft Antimalware automatically updates malicious code signatures by default.

Configuration Evidence

CFG-AVDWindowsUpdateForBusiness-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

CFG-VulnerabilityScans-INT
- Microsoft Defender Portal > Endpoints > Configuration Management > Endpoint Security Policies

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

WUR-WindowsUpdateRing-INT
- Intune Portal > Devices > Management > Windows Updates

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.3		Role Separation
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Separate user functionality from system management functionality.

Procedure Summary

[a]	The Govern Team documents user functionality in the Role Separation Section in the 3.13 System and Communications Protection Policy.
[b]	The Govern Team documents system management functionality in the Role Separation Section in the 3.13 System and Communications Protection Policy.
[c]	The System Designer documents user and system management functionality separation in the Role Separation Section in the 3.13 System and Communications Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.3[a]	Implemented

Assessment Objective
User functionality is identified

Program Procedure
The Govern Team documents user functionality in the Role Separation Section in the 3.13 System and Communications Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents the requirements for role separation and the definitions of user and system management functionality in the Role Separation Section in the 3.13 System and Communications Protection Policy.

Process Evidence

Role Separation Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.3[b]	Implemented

Assessment Objective

System management functionality is identified

Program Procedure

The Govern Team documents system management functionality in the Role Separation Section in the 3.13 System and Communications Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents the requirements for role separation and the definitions of user and system management functionality in the Role Separation Section in the 3.13 System and Communications Protection Policy.

Process Evidence

Role Separation Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.3[c]	Implemented

Assessment Objective

User functionality is separated from system management functionality

Program Procedure

The System Designer documents user and system management functionality separation in the Role Separation Section in the 3.13 System and Communications Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team

Process Summary

- The Govern Team documents user and system management functionality separation in the Role Separation Section in the 3.13 System and Communications Protection Policy.

Process Evidence

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.4		Shared Resource Control
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Prevent unauthorized and unintended information transfer via shared system resources.

Procedure Summary

[a]	The System Deployer configures the system such that unintended information transfer via shared system resources is prevented according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.4[a]	Implemented

Assessment Objective

Unauthorized and unintended information transfer via shared system resources is prevented

Program Procedure

The System Deployer configures the system such that unintended information transfer via shared system resources is prevented according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

Win 10/11 AVD

- Admins assigned to the "Virtual Machine Administrator Login" Role may perform local admin tasks on the AVD by default
- Users assigned to the "Virtual Machine User Login" RBAC Role may sign and use the AVD, but may not use local admin permissions by default

Configuration Evidence

AVD RBAC Roles

- Azure > Resource Groups > [AVD Resource Group] > [Example AVD] > Access Control (IAM) > Role Assignments

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.5		Public-Access System Separation
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Procedure Summary

[a]	The Govern Team defines that publicly accessible systems hosted by the organization are not permitted in the environment in the Public-Access System Separation Section in the 3.13 System and Communications Protection Policy.
[b]	The Govern Team defines that publicly accessible systems hosted by the organization are not allowed in the environment in the Public-Access System Separation Section in the 3.13 System and Communications Protection Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.5[a]	Implemented

Assessment Objective

Publicly accessible system components are identified

Program Procedure

The Govern Team defines that publicly accessible systems hosted by the organization are not permitted in the environment in the Public-Access System Separation Section in the 3.13 System and Communications Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines that publicly accessible systems hosted by the organization are not permitted in the environment.
- The Govern Team documents that publicly accessible systems hosted by the organization are not permitted in the environment in the Public-Access System Separation Section in the 3.13 System and Communications Protection Policy.

Process Evidence

Public-Access System Separation Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.5[b]	Implemented

Assessment Objective

Subnetworks for publicly accessible system components are physically or logically separated from internal networks

Program Procedure

The Govern Team defines that publicly accessible systems hosted by the organization are not allowed in the environment in the Public-Access System Separation Section in the 3.13 System and Communications Protection Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director determines that publicly accessible systems hosted by the organization are not permitted in the environment.
- The Govern Team documents that publicly accessible systems hosted by the organization are not permitted in the environment in the Public-Access System Separation Section in the 3.13 System and Communications Protection Policy.

Process Evidence

Public-Access System Separation Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.6		Network Communication By Exception
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Procedure Summary

[a]	The System Deployer configures the appropriate systems to block network traffic by default according to the System Baseline Standard.
[b]	The System Deployer configures the appropriate systems to allow network traffic by exception according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.6[a]	Implemented

Assessment Objective

Network communications traffic is denied by default

Program Procedure

The System Deployer configures the appropriate systems to block network traffic by default according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Create Named Location LOC-UntrustedLocations-ENT as a blocklist for conditional access policies
- Microsoft maintains deny-by-default, allow by exception network rules in its datacenters by default

Win 10/11 AVD

- Configure CFG-TamperProtection-INT to enable Microsoft recommended antivirus settings (including real-time scans) and disable the ability for attackers to change them.
- Configure SCR-WinFirewallDenyByDefault-INT to deny inbound and outbound traffic by default.

Win 10/11 Win365

- Configure CFG-TamperProtection-INT to enable Microsoft recommended antivirus settings (including real-time scans) and disable the ability for attackers to change them.

Configuration Evidence

CFG-TamperProtection-INT
- Intune > Devices > Manage Devices > Configuration

LOC-UntrustedLocations-ENT
- Azure > Entra ID Conditional Access Policies > Manage > Named Locations

Microsoft FedRAMP SSP
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

SCR-WinFirewallDenyByDefault-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.6[b]	Implemented

Assessment Objective

Network communications traffic is allowed by exception

Program Procedure

The System Deployer configures the appropriate systems to allow network traffic by exception according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft maintains deny-by-default, allow by exception network rules in its datacenters by default

Win 10/11 AVD

- Configure SCR-WinFirewallDenyByDefault-INT to deny inbound and outbound traffic by default.

Configuration Evidence

Microsoft FedRAMP SSP

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

SCR-WinFirewallDenyByDefault-INT

- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.7		Split Tunneling
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

Procedure Summary

[a]	The Govern Team documents that there are no VPNs present in the environment.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.7[a]	Implemented

Assessment Objective

Remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling)

Program Procedure

The Govern Team documents that there are no VPNs present in the environment.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents that there are no VPNs present in the environment.

Process Evidence

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.8		Data In Transit
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

Procedure Summary

[a]	The Govern Team identifies the cryptographic mechanisms for CUI in the Scope Enclave and CUI Flow Diagram.
[b]	The Govern Team identifies that no physical facilities are authorized in the environment.
[c]	The System Deployer configures systems such that CUI is protected in transit according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.8[a]	Implemented

Assessment Objective

Cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified

Program Procedure

The Govern Team identifies the cryptographic mechanisms for CUI in the Scope Enclave and CUI Flow Diagram.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for data in transit in the Data in Transit Section in the 3.13 System and Communications Protection Policy.
- The System Designer describes the cryptographic mechanisms.
- The Govern Team illustrates the cryptographic mechanisms for CUI in the Scope Enclave and CUI Flow Diagram.

Process Evidence

Data in Transit Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.8[b]	Implemented

Assessment Objective

Alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified

Program Procedure

The Govern Team identifies that no physical facilities are authorized in the environment.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents that no physical facilities are authorized within the environment in the Scope Enclave and CUI Flow Diagram.

Process Evidence

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.8[c]	Implemented

Assessment Objective

Either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission

Program Procedure

The System Deployer configures systems such that CUI is protected in transit according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 AVD

- Configure Intune device configuration policy CFG-EnforceFIPSMode-INT to enforce FIPS compliance on endpoints at the Windows operating system level
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Configure Intune device configuration policy CFG-EnforceFIPSMode-INT to enforce FIPS compliance on endpoints at the Windows operating system level
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Configuration Evidence

CFG-EnforceFIPSMode-INT

- Microsoft Intune Admin Center > Devices > Managed Devices > Configuration > Policies

Technical Reference Details About Encryption Learn Article

- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.9		Connections Termination
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Procedure Summary

[a]	The System Designer identifies the period of inactivity for network sessions to terminate as no more than sixty (60) minutes in the System Baseline Standard.
[b]	The System Deployer configures systems such that network connections terminate at the end of sessions according to the System Baseline Standard.
[c]	The System Deployer configures systems such that network connections terminate after no more than sixty (60) minutes of inactivity according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.9[a]	Implemented

Assessment Objective

A period of inactivity to terminate network connections associated with communications sessions is defined

Program Procedure

The System Designer identifies the period of inactivity for network sessions to terminate as no more than sixty (60) minutes in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer Technical Lead

Process Summary

- The Technical Lead determines a period of inactivity for network sessions to terminate as no more than sixty (60) minutes.
- The Govern Team documents that network connections to systems must be terminated when sessions are ended.
- The Govern Team documents the period of inactivity for network sessions to terminate as no more than sixty (60) minutes in the Connection Termination Section in the 3.13 System and Communications Protection Policy.
- The System Designer develops the configurations for a period of inactivity for network sessions to terminate as no more than sixty (60) minutes.

Process Evidence

Connection Termination Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.1 Access Control Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.9[b]	Implemented

Assessment Objective

Network connections associated with communications sessions are terminated at the end of the sessions

Program Procedure

The System Deployer configures systems such that network connections terminate at the end of sessions according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Idle Session Timeout in the M365 admin center to sign users automatically out of Microsoft 365 web apps after sixty (60) minutes.
- Microsoft deallocates TCP ports after four (4) minutes by default.
- Set the Directory Level Idle Timeout in Azure to sixty (60) minutes.

Win 10/11 AVD

- Configure "CFG-RequireSMBSigning-INT" to enforce SMB packet signing and mitigate SMB relay attacks.
- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes
- Microsoft deallocates TCP ports after four (4) minutes by default.

Win 10/11 Win365

- Configure "CFG-RequireSMBSigning-INT" to enforce SMB packet signing and mitigate SMB relay attacks.
- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes
- Microsoft deallocates TCP ports after four (4) minutes by default.

Configuration Evidence

CFG-DisconnectIdleRemoteSessions-INT

- Go to Intune Admin Center → Devices → Configuration

CFG-RemoveIdleDisconnectedSessions-INT

- Go to Intune Admin Center → Devices → Configuration

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

CFG-RequireSMBSigning-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Directory Level Idle Timeout
- Azure > Top Right Settings Cog > Signing Out + Notifications > Enable Directory Level Timeout

Idle Session Timeout
- Microsoft Admin Center (portal.office365.us/adminportal) > Settings > Org Settings > Security and Privacy > Idle Session Timeout

Windows OS (TCP Port Release Timeout)
- https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/tcp-ip-connectivity-issues-troubleshooting#introduction-of-tcp

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.9[c]	Implemented

Assessment Objective

Network connections associated with communications sessions are terminated after the defined period of inactivity

Program Procedure

The System Deployer configures systems such that network connections terminate after no more than sixty (60) minutes of inactivity according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Idle Session Timeout in the M365 admin center to sign users automatically out of Microsoft 365 web apps after sixty (60) minutes.
- Microsoft deallocates TCP ports after four (4) minutes by default.
- Set the Directory Level Idle Timeout in Azure to sixty (60) minutes.

Win 10/11 AVD

- Configure "CFG-RequireSMBSigning-INT" to enforce SMB packet signing and mitigate SMB relay attacks.
- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes
- Microsoft deallocates TCP ports after four (4) minutes by default.

Win 10/11 Win365

- Configure "CFG-RequireSMBSigning-INT" to enforce SMB packet signing and mitigate SMB relay attacks.
- Configure CFG-DisconnectIdleRemoteSessions-INT to disconnect inactive users on remote sessions after sixty (60) minutes.
- Configure CFG-RemoveIdleDisconnectedSessions-INT to sign out and shut down disconnected AVD sessions after thirty (30) minutes
- Microsoft deallocates TCP ports after four (4) minutes by default.

Configuration Evidence

CFG-DisconnectIdleRemoteSessions-INT

- Go to Intune Admin Center → Devices → Configuration

CFG-RemoveIdleDisconnectedSessions-INT

- Go to Intune Admin Center → Devices → Configuration

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

CFG-RequireSMBSigning-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Directory Level Idle Timeout
- Azure > Top Right Settings Cog > Signing Out + Notifications > Enable Directory Level Timeout

Idle Session Timeout
- Microsoft Admin Center (portal.office365.us/adminportal) > Settings > Org Settings > Security and Privacy > Idle Session Timeout

Windows OS (TCP Port Release Timeout)
- https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/tcp-ip-connectivity-issues-troubleshooting#introduction-of-tcp

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.10		Key Management
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Establish and manage cryptographic keys for cryptography employed in organizational systems.

Procedure Summary

[a]	The System Designer documents that cryptographic keys are established whenever cryptography is employed in the System Baseline Standard.
[b]	The System Deployer configures the system such that cryptographic keys are managed whenever cryptography is employed according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.10[a]	Implemented

Assessment Objective

Cryptographic keys are established whenever cryptography is employed

Program Procedure

The System Designer documents that cryptographic keys are established whenever cryptography is employed in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents that cryptographic keys are established whenever cryptography is employed in the Key Management Section in the 3.13 System and Communications Protection Policy.
- The System Designer develops configurations such that cryptographic keys are established whenever cryptography is employed.
- The System Designer documents the configurations that establish cryptographic keys whenever cryptography is employed in the System Baseline Standard.

Process Evidence

Key Management Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.10[b]	Implemented

Assessment Objective

Cryptographic keys are managed whenever cryptography is employed

Program Procedure

The System Deployer configures the system such that cryptographic keys are managed whenever cryptography is employed according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft manages cryptographic keys for Microsoft datacenters by default
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 AVD

- Azure Virtual Machines are encrypted by default
- Microsoft backs up BitLocker recovery keys to Entra by default
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Microsoft backs up BitLocker recovery keys to Entra by default
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Configuration Evidence

Azure Virtual Machine Disk Encryption

- Azure > Virtual Machines > (example virtual machine) > Settings > Disks > (example disk) > Settings > Encryption > (Default) Encryption at-rest with a platform managed key

Microsoft Backup BitLocker Keys Learn Article

- https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/recovery-process#helpdesk-recovery

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Technical Reference Details About Encryption Learn Article

- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.11		CUI Encryption
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Procedure Summary

[a]	The System Deployer configures the system such that FIPS validated encryption is used to protect CUI.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.11[a]	Implemented

Assessment Objective

Fips-validated cryptography is employed to protect the confidentiality of CUI

Program Procedure

The System Deployer configures the system such that FIPS validated encryption is used to protect CUI.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 AVD

- Azure Virtual Machines are encrypted by default
- Configure Intune device configuration policy CFG-EnforceFIPSMode-INT to enforce FIPS compliance on endpoints at the Windows operating system level
- Microsoft applies FIPS validated encryption to endpoints at the drive layer in the datacenter
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Configure Intune device configuration policy CFG-EnforceFIPSMode-INT to enforce FIPS compliance on endpoints at the Windows operating system level
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.
- Windows 365 PCs use Azure FIPS-validated encryption by default

Configuration Evidence

Azure Virtual Machine Disk Encryption

- Azure > Virtual Machines > (example virtual machine) > Settings > Disks > (example disk) > Settings > Encryption > (Default) Encryption at-rest with a platform managed key

CFG-EnforceFIPSMode-INT

- Microsoft Intune Admin Center > Devices > Managed Devices > Configuration > Policies

Cryptography API: Next Generation Microsoft Learn Article

- https://learn.microsoft.com/en-us/windows/win32/seccng/cng-features#certification-and-compliance

Technical Reference Details About Encryption Learn Article

- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

Windows 365 Encryption Learn Article

- https://learn.microsoft.com/en-za/windows-365/enterprise/encryption#encryption-of-data-at-rest

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.12		Collaborative Device Control
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

Procedure Summary

[a]	The Govern Team documents that no collaborative computing devices are in scope in the environment.
[b]	The Govern Team documents that no collaborative computing devices are in scope in the environment.
[c]	The Govern Team documents that no collaborative computing devices are in scope in the environment.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.12[a]	Implemented

Assessment Objective

Collaborative computing devices are identified

Program Procedure

The Govern Team documents that no collaborative computing devices are in scope in the environment.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents that no collaborative computing devices are in scope in the environment.

Process Evidence

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.12[b]	Implemented

Assessment Objective

Collaborative computing devices provide indication to users of devices in use

Program Procedure

The Govern Team documents that no collaborative computing devices are in scope in the environment.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents that no collaborative computing devices are in scope in the environment.

Process Evidence

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.12[c]	Implemented

Assessment Objective

Remote activation of collaborative computing devices is prohibited

Program Procedure

The Govern Team documents that no collaborative computing devices are in scope in the environment.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team

Process Summary

- The Govern Team documents that no collaborative computing devices are in scope in the environment.

Process Evidence

Scope Enclave and CUI Flow Diagram
- SharePoint > Govern Docs > Artifacts > Scope Enclave and CUI Flow Diagram

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.13		Mobile Code
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Control and monitor the use of mobile code.

Procedure Summary

[a]	The System Deployer configures systems such that mobile code is controlled according to the System Baseline Standard.
[b]	The System Security Analyst monitors for the use of mobile code in the Security Monitoring Output Log.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.13[a]	Implemented

Assessment Objective

Use of mobile code is controlled

Program Procedure

The System Deployer configures systems such that mobile code is controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Attack Surface Reduction Policy ASR-BlockMalCodeExecution-INT to block the use of malicious code

Win 10/11 AVD

- Configure Attack Surface Reduction Policy ASR-BlockMalCodeExecution-INT to block the use of malicious code

Win 10/11 Win365

- Configure Attack Surface Reduction Policy ASR-BlockMalCodeExecution-INT to block the use of malicious code

Configuration Evidence

ASR-BlockMalCodeExecution-INT

- Azure Admin Portal > Intune > Endpoint Security > Manage > Attack Surface Reduction

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.13[b]	Implemented

Assessment Objective

Use of mobile code is monitored

Program Procedure

The System Security Analyst monitors for the use of mobile code in the Security Monitoring Output Log.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Configure Sentinel Analytic rule SAR-ActiveXEvent-SEN to detect ActiveX execution on endpoints.
- Configure Sentinel Analytic rule SAR-FlashEvent-SEN to detect flash execution on endpoints.
- Configure Sentinel Analytic rule SAR-JavaEvent-SEN to detect Java execution on endpoints.
- Configure Sentinel Analytic rule SAR-JavaScriptEvent-SEN to detect JavaScript execution on endpoints.
- Configure Sentinel Analytic rule SAR-PDFEvent-SEN to detect PDF execution on endpoints.
- Configure Sentinel Analytic rule SAR-PostScriptEvent-SEN to detect PostScript execution on endpoints.
- Configure Sentinel Analytic rule SAR-VBScriptEvent-SEN to detect VBScript execution on endpoints.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default
- Microsoft Sentinel provides audit reduction and report generation by default

Win 10/11 AVD

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Win 10/11 Win365

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Configuration Evidence

EDR-DeployDefenderConnector-INT

- Intune Portal > Endpoint Security > Endpoint Detection and Response

Microsoft Defender XDR to Sentinel Connector Learn Article

- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

SAR-ActiveXEvent-SEN
- Sentinel > Configuration > Analytics

SAR-FlashEvent-SEN
- Sentinel > Configuration > Analytics

SAR-JavaEvent-SEN
- Sentinel > Configuration > Analytics

SAR-JavaScriptEvent-SEN
- Sentinel > Configuration > Analytics

SAR-PDFEvent-SEN
- Sentinel > Configuration > Analytics

SAR-PostScriptEvent-SEN
- Sentinel > Configuration > Analytics

SAR-VBScriptEvent-SEN
- Sentinel > Configuration > Analytics

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.14		Voice Over Internet Protocol
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

Procedure Summary

[a]	The System Deployer configures the system such that VOIP technologies are controlled according to the System Baseline Standard.
[b]	The System Security Analyst monitors VOIP systems for unauthorized use.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.14[a]	Implemented

Assessment Objective

Use of Voice over Internet Protocol (VoIP) technologies is controlled

Program Procedure

The System Deployer configures the system such that VOIP technologies are controlled according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft controls VOIP sessions by default

Configuration Evidence

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.14[b]	Implemented

Assessment Objective

Use of Voice over Internet Protocol (VoIP) technologies is monitored

Program Procedure

The System Security Analyst monitors VOIP systems for unauthorized use.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default

Win 10/11 AVD

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Win 10/11 Win365

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Configuration Evidence

EDR-DeployDefenderConnector-INT

- Intune Portal > Endpoint Security > Endpoint Detection and Response

Microsoft Defender XDR to Sentinel Connector Learn Article

- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.15		Communications Authenticity
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement
Protect the authenticity of communications sessions.

Procedure Summary	
[a]	The System Deployer configures the system such that the authenticity of communications sessions is protected according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.15[a]	Implemented

Assessment Objective

The authenticity of communications sessions is protected

Program Procedure

The System Deployer configures the system such that the authenticity of communications sessions is protected according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.
- Microsoft uses TLS encryption to protect the authenticity of communication sessions by default.

Win 10/11 AVD

- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares
- Configure "CFG-RequireSMBSigning-INT" to enforce SMB packet signing and mitigate SMB relay attacks.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Win 10/11 Win365

- Configure "CFG-DisallowNullSessions-INT" to disallow unauthenticated network connections to servers and network shares
- Configure "CFG-RequireSMBSigning-INT" to enforce SMB packet signing and mitigate SMB relay attacks.
- Configure Conditional Access Policy CAP-EnforceRRMFA-EID to require authentication using a replay-resistant MFA method for all users accessing cloud resources.
- Microsoft uses FIPS-validated encryption for data at rest and in transit by default.

Configuration Evidence

CAP-EnforceRRMFA-EID

- Entra Admin Portal > Security > Conditional Access

CFG-DisallowNullSessions-INT

- Intune > Devices > Manage Devices > Configuration

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

CFG-RequireSMBSigning-INT

- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Technical Reference Details About Encryption Learn Article

- https://learn.microsoft.com/en-us/purview/technical-reference-details-about-encryption

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SC.L2-3.13.16		Data At Rest
SPRS Value	**SPRS Score**	**Practice Status**
1	1	**Implemented**

Practice Statement

Protect the confidentiality of CUI at rest.

Procedure Summary

[a]	The System Deployer configures the tenant such that devices that store CUI are not permitted to connect according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.13.16[a]	Implemented

Assessment Objective
The confidentiality of CUI at rest is protected

Program Procedure
The System Deployer configures the tenant such that devices that store CUI are not permitted to connect according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Process	System Deployer	Govern Team

Process Summary

- The Govern Team documents that devices that store CUI at rest are not permitted in the enclave in the Data at Rest Section in the 3.13 System and Communications Protection Policy.

Process Evidence

Data at Rest Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.13 System and Communications Protection Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SI.L2-3.14.1		Flaw Remediation
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Identify, report, and correct information and information system flaws in a timely manner.

Procedure Summary

[a]	The Govern Team defines the time within which to identify system flaws in the Flaw Remediation Section in the 3.14 System and Information Integrity Policy.
[b]	The System Security Analyst identifies system flaws within sixty (60) days.
[c]	The Govern Team defines the time within which to report system flaws in the Flaw Remediation Section in the 3.14 System and Information Integrity Policy.
[d]	The System Security Analyst reports system flaws by creating a Maintenance Case within sixty (60) days.
[e]	The Govern Team defines the time within which to correct system flaws in the Flaw Remediation Section in the 3.14 System and Information Integrity Policy.
[f]	The System Maintainer corrects the system flaws using the patch management process within 30 days for critical, sixty (60) days for high, 90 for medium and 180 for low vulnerabilities.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.1[a]	Implemented

Assessment Objective

The time within which to identify system flaws is specified

Program Procedure

The Govern Team defines the time within which to identify system flaws in the Flaw Remediation Section in the 3.14 System and Information Integrity Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director defines the time within which to identify system flaws to be sixty (60) days.
- The Govern Team documents the time within which to identify system flaws to be sixty (60) days in the Flaw Remediation Section in the 3.14 System and Information Integrity Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Flaw Remediation Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.14 System and Information Integrity Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.1[b]	Implemented

Assessment Objective

System flaws are identified within the specified time frame

Program Procedure

The System Security Analyst identifies system flaws within sixty (60) days.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Defend Team	Defend Team

Configuration Summary

M365 GCC-H

- Microsoft identifies, reports, and corrects on system flaws in the tenant by default.

Qualys

- A Qualys Patch Management Agent is deployed to scan for, and automatically remediate vulnerabilities via patches made available by vendors.

Win 10/11 AVD

- Configure an Automation Account within Azure to start AVDs on Friday morning for patch cycle.
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.

Win 10/11 Win365

- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.

Configuration Evidence

Automation Account for Patch
- Azure portal > Automation Account

M365 Service Health Alerts
- Microsoft Admin Center (portal.office365.us/adminportal) > Show all > Health > Service Health > Customize > Email

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

Qualys Agent Dashboard
- Qualys > Agent Dashboard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.1[c]	Implemented

Assessment Objective

The time within which to report system flaws is specified

Program Procedure

The Govern Team defines the time within which to report system flaws in the Flaw Remediation Section in the 3.14 System and Information Integrity Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director defines the time within which to report system flaws to be sixty (60) days.
- The Govern Team documents the time within which to report system flaws to be sixty (60) days in the Flaw Remediation Section in the 3.14 System and Information Integrity Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Flaw Remediation Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.14 System and Information Integrity Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.1[d]	Implemented

Assessment Objective

System flaws are reported within the specified time frame

Program Procedure

The System Security Analyst reports system flaws by creating a Maintenance Case within sixty (60) days.

Procedure Type	Responsible Role	Supporting Roles
Process	System Security Analyst	System Maintainer System Security Analyst

Process Summary

- The System Security Analyst reviews the Patch Management tool for vulnerabilities.
- The System Security Analyst opens a Maintenance Case for each Critical and High Vulnerability found.
- The System Security Analyst assigns the Maintenance Case to the System Maintainer.
- The System Maintainer patches the vulnerability if there is a patch available.
- The System Maintainer escalates the Maintenance Case to the Escalation Support Team if there is not a patch available.
- The System Maintainer updates and closes the Maintenance Case.

Process Evidence

Maintenance Case
- support.ardalyst.com

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Assessment Objective Identifier	Assessment Objective Status
3.14.1[e]	Implemented

Assessment Objective

The time within which to correct system flaws is specified

Program Procedure

The Govern Team defines the time within which to correct system flaws in the Flaw Remediation Section in the 3.14 System and Information Integrity Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Cybersecurity Program Director Govern Team

Process Summary

- The Cybersecurity Program Director defines the time within which to correct system flaws to be thirty (30) days for critical, sixty (60) for high, ninety (90) for medium and one hundred eighty (180) for low.
- The Govern Team documents the time within which to correct system flaws to be thirty (30) days for critical, sixty (60) for high, ninety (90) for medium and one hundred eighty (180) for low in the Flaw Remediation Section in the 3.14 System and Information Integrity Policy.

Process Evidence

Cybersecurity Policy Manual
- SharePoint > Govern Docs > Artifacts > Cybersecurity Policy Manual

Flaw Remediation Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.14 System and Information Integrity Policy

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.1[f]	Implemented

Assessment Objective

System flaws are corrected within the specified time frame

Program Procedure

The System Maintainer corrects the system flaws using the patch management process within thirty (30) days for critical, sixty (60) for high, ninety (90) for medium and one hundred eighty (180) for low.

Procedure Type	Responsible Role	Supporting Roles
Process	System Maintainer	System Maintainer System Security Analyst

Process Summary

- The System Security Analyst reviews the Patch Management tool for vulnerabilities.
- The System Security Analyst opens a Maintenance Case for each Critical and High Vulnerability found.
- The System Security Analyst assigns the Maintenance Case to the System Maintainer.
- The System Maintainer patches the vulnerability if there is a patch available.
- The System Maintainer escalates the Maintenance Case to the Escalation Support Team if there is not a patch available.
- The System Maintainer updates and closes the Maintenance Case.
- The System Security Analyst documents patch reports which display remediations, patches, and known vulnerabilities

Process Evidence

Maintenance Case
- support.ardalyst.com

Patch Report
- SharePoint > Govern Docs > Artifacts > Patch Report

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SI.L2-3.14.2		Malicious Code Protection
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Provide protection from malicious code at designated locations within organizational systems.

Procedure Summary

[a]	The System Designer identifies the locations for malicious code protection in the System Catalog.
[b]	The System Deployer configures the system such that protection from malicious code at designated locations is provided according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.2[a]	Implemented

Assessment Objective

Designated locations for malicious code protection are identified

Program Procedure

The System Designer identifies the locations for malicious code protection in the System Catalog.

Procedure Type	Responsible Role	Supporting Roles
Process	System Designer	Govern Team System Designer

Process Summary

- The Govern Team documents the requirements for malicious code protection in the Malicious Code Protection Section in the 3.14 System and Information Integrity Policy.
- The System Designer documents the mechanism for malicious code protection in the System Catalog.
- The System Designer develops the configuration for malicious code protection.
- The System Designer documents the configuration for malicious code protection in the System Baseline Standard.

Process Evidence

Malicious Code Protection Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.14 System and Information Integrity Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

System Catalog
- SharePoint > Govern Docs > Artifacts > System Catalog

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.2[b]	Implemented

Assessment Objective

Protection from malicious code at designated locations is provided

Program Procedure

The System Deployer configures the system such that protection from malicious code at designated locations is provided according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Win 10/11 AVD

- Configure "Connect Windows Devices to Microsoft Defender for Endpoint" in Microsoft Intune
- Configure "Microsoft Intune Connection" in Microsoft Defender
- Configure "SCR-DisableAutoPlayForDefaultUserProfileOnWindowsDevices-INT" to disable Autoplay in the Default User Profile template on Windows devices.
- Configure "SCR-DisableWindowsAutoPlayOnWindowsDevices-INT" to disable Windows Explorer Autoplay on Windows devices.
- Configure "SCR-EnableSignaturePadding-INT" to enable WinVerifyTrust digital signature padding on managed Windows devices
- Configure CFG-TamperProtection-INT to enable Microsoft recommended antivirus settings (including real-time scans) and disable the ability for attackers to change them.
- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.

Win 10/11 Win365

- Configure "Connect Windows Devices to Microsoft Defender for Endpoint" in Microsoft Intune
- Configure "Microsoft Intune Connection" in Microsoft Defender
- Configure "SCR-DisableAutoPlayForDefaultUserProfileOnWindowsDevices-INT" to disable Autoplay in the Default User Profile template on Windows devices.
- Configure "SCR-DisableWindowsAutoPlayOnWindowsDevices-INT" to disable Windows Explorer Autoplay on Windows devices.
- Configure "SCR-EnableSignaturePadding-INT" to enable WinVerifyTrust digital signature padding on managed Windows devices

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- Configure CFG-TamperProtection-INT to enable Microsoft recommended antivirus settings (including real-time scans) and disable the ability for attackers to change them.
- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.

Configuration Evidence

CFG-TamperProtection-INT
- Intune > Devices > Manage Devices > Configuration

Defender for Endpoint Windows Connector
- Intune > Endpoint Security > Setup > Microsoft Defender for Endpoint > "Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint"

EDR-DeployDefenderConnector-INT
- Intune Portal > Endpoint Security > Endpoint Detection and Response

Microsoft Intune Connection
- Defender > System > Settings > Endpoints > General > Advanced Features > "Microsoft Intune Connection" > "On"

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

SCR-DisableWindowsAutoPlayOnWindowsDevices-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

SCR-EnableSignaturePadding-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

SRC-DisableAutoPlayForDefaultUserProfileOnWindowsDevices-INT
- Intune > Devices > Manage Devices > Scripts and Remediations > Remediations

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SI.L2-3.14.3		Security Alerts and Advisories
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Monitor system security alerts and advisories and take action in response.

Procedure Summary

[a]	The Defend Team identifies response actions to advisories or intelligence in the Weekly Cyber Intel Newsletter and the Emergent Intel Advisory.
[b]	The Defend Team monitors advisories and intelligence during the News Review Process.
[c]	The Defend Team opens Change Control Request Cases during the News Review process so actions are taken to advisories and intelligence.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.3[a]	Implemented

Assessment Objective

Response actions to system security alerts and advisories are identified

Program Procedure

The Defend Team identifies response actions to advisories or intelligence in the Weekly Cyber Intel Newsletter and the Emergent Intel Advisory.

Procedure Type	Responsible Role	Supporting Roles
Process	Defend Team	Defend Team

Process Summary

- The Defend Team documents relevant articles in the Weekly Cyber Intel Newsletter.
- The Defend Team summarizes relevant articles in the Weekly Cyber Intel Newsletter.
- The Defend Team documents emergent articles in the Emergent Intel Advisory.
- The Defend Team summarizes emergent articles in the Emergent Intel Advisory.

Process Evidence

Emergent Intel Advisory
- SharePoint > Govern Docs > Artifacts > Emergent Intel Advisory

Weekly Cyber Intel Newsletter
- SharePoint > Govern Docs > Artifacts > Weekly Cyber Intel Newsletter

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.3[b]	Implemented

Assessment Objective

System security alerts and advisories are monitored

Program Procedure

The Defend Team monitors advisories and intelligence during the News Review Process.

Procedure Type	Responsible Role	Supporting Roles
Process	Defend Team	Defend Team Govern Team

Process Summary

- The Govern Team documents the requirements for news review in the Security Alerts and Advisories Section in the 3.12 Security Assessment Policy.
- The Defend Team creates the Tesseract Intel Sources List.
- The Defend Team reviews the Tesseract Intel Sources List.
- The Defend Team monitors the Tesseract Intel Sources List.

Process Evidence

Security Alerts and Advisories Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.14 System and Information Integrity Policy

Tesseract Intel Sources List
- SharePoint > Govern Docs > Artifacts > Tesseract Intel Sources List

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.3[c]	Implemented

Assessment Objective

Actions in response to system security alerts and advisories are taken

Program Procedure

The Defend Team opens Change Control Request Cases during the News Review process so actions are taken to advisories and intelligence.

Procedure Type	Responsible Role	Supporting Roles
Process	Defend Team	Defend Team

Process Summary

- For routine alerts and advisories, the Defend Team documents required actions for relevant articles in the Weekly Cyber Intel Newsletter.
- The Defend Team opens a Change Control Request Case for relevant articles.
- The Defend Team publishes the Weekly Cyber Intel Newsletter at the end of the week following the publication review process.
- For emergent issues, the Defend Team completes all the fields in the News Review Log to record completion of News Review.
- The Defend Team documents required actions for emergent articles in the Emergent Intel Advisory.
- The Defend Team opens a Change Control Request Case for emergent articles.
- The Defend Team publishes the Emergent Intel Advisory on the same day as detection following the publication review process.
- The Defend Team completes all the fields in the News Review Log to record completion of News Review.

Process Evidence

Change Control Request Case
- support.ardalyst.com

Emergent Intel Advisory
- SharePoint > Govern Docs > Artifacts > Emergent Intel Advisory

News Review Log
- SharePoint > Govern Docs > Artifacts > News Review Log

Weekly Cyber Intel Newsletter
- SharePoint > Govern Docs > Artifacts > Weekly Cyber Intel Newsletter

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SI.L2-3.14.4		Update Malicious Code Protection
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Update malicious code protection mechanisms when new releases are available.

Procedure Summary

[a]	The System Deployer configures systems such that they update malicious code protection mechanisms when new releases are available according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.4[a]	Implemented

Assessment Objective

Malicious code protection mechanisms are updated when new releases are available

Program Procedure

The System Deployer configures systems such that they update malicious code protection mechanisms when new releases are available according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

Win 10/11 AVD

- Configure CFG-AVDWindowsUpdateForBusiness-INT to implement forced updates on AVD.
- Microsoft Antimalware automatically updates malicious code signatures by default.

Win 10/11 Win365

- Configure Windows Update Ring WUR-WindowsUpdateRing-INT to enforce Windows updates on managed endpoints
- Microsoft Antimalware automatically updates malicious code signatures by default.

Configuration Evidence

CFG-AVDWindowsUpdateForBusiness-INT
- Microsoft Intune Portal > Devices > Manage Devices > Configuration > Policies

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

WUR-WindowsUpdateRing-INT
- Intune Portal > Devices > Management > Windows Updates

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SI.L2-3.14.5		System and File Scanning
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

Procedure Summary

[a]	The Govern Team defines the frequency for malicious code scans as no more than thirty (30) days in the System and File Scanning Section in the 3.14 System and Information Integrity Policy.
[b]	The System Deployer configures systems such that they perform malicious code scans according to the frequency in the System Baseline Standard.
[c]	The System Deployer configures systems such that they perform malicious code scans on file download, open, and execute according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.5[a]	Implemented

Assessment Objective

The frequency for malicious code scans is defined

Program Procedure

The Govern Team defines the frequency for malicious code scans as no more than thirty (30) days in the System and File Scanning Section in the 3.14 System and Information Integrity Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Govern Team System Designer

Process Summary

- The Govern Team documents the frequency for malicious code scans as no more than thirty (30) days in the System and File Scanning Section in the 3.14 System and Information Integrity Policy.
- The System Designer develops the configurations for the frequency of malicious code scans.
- The System Designer documents the configurations for the frequency of malicious code scans in the System Baseline Standard.

Process Evidence

System and File Scanning Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.14 System and Information Integrity Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.5[b]	Implemented

Assessment Objective

Malicious code scans are performed with the defined frequency

Program Procedure

The System Deployer configures systems such that they perform malicious code scans according to the frequency in the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft provides malicious code scans of the tenant by default.

Win 10/11 AVD

- Configure CFG-TamperProtection-INT to enable Microsoft recommended antivirus settings (including real-time scans) and disable the ability for attackers to change them.
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.

Win 10/11 Win365

- Configure CFG-TamperProtection-INT to enable Microsoft recommended antivirus settings (including real-time scans) and disable the ability for attackers to change them.
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.

Configuration Evidence

CFG-TamperProtection-INT

- Intune > Devices > Manage Devices > Configuration

M365 Malware Protection Learn Article

- https://learn.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.5[c]	Implemented

Assessment Objective

Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed

Program Procedure

The System Deployer configures systems such that they perform malicious code scans on file download, open, and execute according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Microsoft enables "Safe Attachments" real-time scanning by default
- Microsoft provides malicious code scans of the tenant by default.

Win 10/11 AVD

- Configure CFG-TamperProtection-INT to enable Microsoft recommended antivirus settings (including real-time scans) and disable the ability for attackers to change them.
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.

Win 10/11 Win365

- Configure CFG-TamperProtection-INT to enable Microsoft recommended antivirus settings (including real-time scans) and disable the ability for attackers to change them.
- Microsoft Defender for Endpoint automatically scans devices to identify flaws and vulnerabilities by default.

Configuration Evidence

CFG-TamperProtection-INT
- Intune > Devices > Manage Devices > Configuration

M365 Malware Protection Learn Article
- https://learn.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection

Microsoft Safe Attachments Learn Article
- https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-about

Microsoft Technical Reference Guide
- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SI.L2-3.14.6		Monitor Communications For Attacks
SPRS Value	**SPRS Score**	**Practice Status**
5	5	**Implemented**

Practice Statement

Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Procedure Summary

[a]	The Defend Team conducts security monitoring according to the Monitor Communications for Attacks Section in the 3.14 System and Information Integrity Policy.
[b]	The System Deployer configures the system such that it detects indicators of potential attacks within inbound communications traffic according to the System Baseline Standard.
[c]	The System Deployer configures the system such that it detects indicators of potential attacks within outbound communications traffic according to the System Baseline Standard.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.6[a]	Implemented

Assessment Objective

The system is monitored to detect attacks and indicators of potential attacks

Program Procedure

The Defend Team conducts security monitoring according to the Monitor Communications for Attacks Section in the 3.14 System and Information Integrity Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Defend Team	Cybersecurity Program Director Defend Team Govern Team System Deployer System Designer

Process Summary

- The Govern Team documents the requirements for security monitoring in the Monitor Communications for Attacks Section in the 3.14 System and Information Integrity Policy.
- The System Designer develops the configuration for the system to detect indicators of potential attacks.
- The System Designer develops configuration for the system to detect indicators of potential attacks within inbound communications traffic.
- The System Designer develops the configuration for the system to detect indicators of potential attacks within outbound communications traffic.
- The System Designer documents the configuration for the system to detect indicators of potential attacks in the System Baseline Standard.
- The System Designer documents the configuration for the system to detect indicators of potential attacks within inbound communications traffic in the System Baseline Standard.
- The System Designer documents the configuration for the system to detect indicators of potential attacks within outbound communications traffic in the System Baseline Standard.
- The System Deployer configures the system such that it detects indicators of potential attacks according to the System Baseline Standard.
- The System Deployer configures the system such that it detects indicators of potential attacks within inbound communications traffic according to the System Baseline Standard.
- The System Deployer configures the system such that it detects indicators of potential attacks within outbound communications traffic according to the System Baseline Standard.
- The Defend Team reviews alerts in the SIEM.
- The Defend Team identifies alerts that need further investigation.
- The Defend Team investigates the alert to determine if it is a suspected threat event.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

- The Defend Team conducts any time sensitive triage actions.
- The Defend Team opens an Event Investigation Case for each alert deemed a suspected threat event.
- The Defend Team notifies the Technical Lead of a suspected threat event.
- The Defend Team investigates the suspected threat event.
- The Defend Team determines if the suspected threat event is a false positive or a true positive.
- The Defend Team closes the Event Investigation Case if it is a false positive.
- The Defend Team remediates if it is a true positive.
- The Defend Team updates the Event Investigation Case if it is a true positive.
- The Defend Team notifies the Cybersecurity Program Director if it is a true positive.
- The Cybersecurity Program Director determines if the True Positive Suspected Threat Event should initiate the Incident Response Plan.
- The Defend Team completes the Security Monitoring Output Log.

Process Evidence

Event Investigation Case
- support.ardalyst.com

Monitor Communications for Attacks Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.14 System and Information Integrity Policy

Security Monitoring Output Log
- SharePoint > Govern Docs > Artifacts > Security Monitoring Output Log

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Assessment Objective Identifier	Assessment Objective Status
3.14.6[b]	Implemented

Assessment Objective

Inbound communications traffic is monitored to detect attacks and indicators of potential attacks

Program Procedure

The System Deployer configures the system such that it detects indicators of potential attacks within inbound communications traffic according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Configure Microsoft Entra ID data connector to send audit, sign in and non-interactive sign in logs to the Log Analytics Workspace.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default
- Microsoft Sentinel provides audit reduction and report generation by default

Win 10/11 AVD

- Configure "Connect Windows Devices to Microsoft Defender for Endpoint" in Microsoft Intune
- Configure "Microsoft Intune Connection" in Microsoft Defender
- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Win 10/11 Win365

- Configure "Connect Windows Devices to Microsoft Defender for Endpoint" in Microsoft Intune
- Configure "Microsoft Intune Connection" in Microsoft Defender
- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Configuration Evidence

Defender for Endpoint Windows Connector

- Intune > Endpoint Security > Setup > Microsoft Defender for Endpoint > "Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint"

EDR-DeployDefenderConnector-INT

- Intune Portal > Endpoint Security > Endpoint Detection and Response

Microsoft Defender XDR to Sentinel Connector Learn Article

- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Microsoft Entra ID Log Diagnostic Settings

- Entra ID > Monitoring > Diagnostic settings

Microsoft Intune Connection

- Defender > System > Settings > Endpoints > General > Advanced Features > "Microsoft Intune Connection" > "On"

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.6[c]	Implemented

Assessment Objective

Outbound communications traffic is monitored to detect attacks and indicators of potential attacks

Program Procedure

The System Deployer configures the system such that it detects indicators of potential attacks within outbound communications traffic according to the System Baseline Standard.

Procedure Type	Responsible Role	Supporting Roles
Configuration	Harden Team	Harden Team

Configuration Summary

M365 GCC-H

- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.
- Microsoft enables the connector between Microsoft Defender for Endpoint and Microsoft Sentinel by default
- Microsoft Sentinel provides audit reduction and report generation by default

Win 10/11 AVD

- Configure "Connect Windows Devices to Microsoft Defender for Endpoint" in Microsoft Intune
- Configure "Microsoft Intune Connection" in Microsoft Defender
- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Win 10/11 Win365

- Configure "Connect Windows Devices to Microsoft Defender for Endpoint" in Microsoft Intune
- Configure "Microsoft Intune Connection" in Microsoft Defender
- Configure Endpoint Detection and Response EDR-DeployDefenderConnector-INT to deploy Defender agents to Windows endpoints.

Configuration Evidence

Defender for Endpoint Windows Connector

- Intune > Endpoint Security > Setup > Microsoft Defender for Endpoint > "Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint"

EDR-DeployDefenderConnector-INT

- Intune Portal > Endpoint Security > Endpoint Detection and Response

Microsoft Defender XDR to Sentinel Connector Learn Article

- https://learn.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender?tabs=MDE

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Microsoft Intune Connection

- Defender > System > Settings > Endpoints > General > Advanced Features > "Microsoft Intune Connection" > "On"

Microsoft Technical Reference Guide

- https://www.microsoft.com/en-us/download/details.aspx?id=103401

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Practice Code		Practice Name
SI.L2-3.14.7		Identify Unauthorized Use
SPRS Value	**SPRS Score**	**Practice Status**
3	3	**Implemented**

Practice Statement

Identify unauthorized use of organizational systems.

Procedure Summary

[a]	The Govern Team documents authorized use requirements in the Identify Unauthorized Use Section in the 3.14 System and Information Integrity Policy.
[b]	The Defend Team monitors for alerts for authorized use according to the Identify Unauthorized Use Section in the 3.14 System and Information Integrity Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.7[a]	Implemented

Assessment Objective

Authorized use of the system is defined

Program Procedure

The Govern Team documents authorized use requirements in the Identify Unauthorized Use Section in the 3.14 System and Information Integrity Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Govern Team	Authorized User Cybersecurity Program Director Govern Team Human Resources Team

Process Summary

- The Govern Team documents the requirements for identifying unauthorized use in the Identify Unauthorized Use Section in the 3.14 System and Information Integrity Policy.
- The Govern Team documents the Acceptable Use Policy.
- The Human Resources Team coordinates the signing of the Acceptable Use Policy.
- The Authorized User signs the Acceptable Use Policy.
- The Cybersecurity Program Director documents the signing of the acceptable use policy in the Training Management System.

Process Evidence

Acceptable Use Policy
- SharePoint > Govern Docs > Artifacts > Acceptable Use Policy

Identify Unauthorized Use Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.14 System and Information Integrity Policy

User, Process, and Asset Inventory
- SharePoint > Govern Docs > Artifacts > User, Process, and Asset Inventory

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Assessment Objective Identifier	Assessment Objective Status
3.14.7[b]	Implemented

Assessment Objective

Unauthorized use of the system is identified

Program Procedure

The Defend Team monitors for alerts for authorized use according to the Identify Unauthorized Use Section in the 3.14 System and Information Integrity Policy.

Procedure Type	Responsible Role	Supporting Roles
Process	Defend Team	Defend Team Govern Team System Deployer System Designer

Process Summary

- The Govern Team documents the requirements for identifying unauthorized use in the Identify Unauthorized Use Section in the 3.14 System and Information Integrity Policy.
- The System Designer develops the configuration for alerting for unauthorized use.
- The System Designer documents the configuration for alerting for unauthorized use in the System Baseline Standard.
- The System Deployer configures the system such that it alerts for unauthorized use according to the System Baseline Standard.
- The Defend Team monitors for alerts for unauthorized use according to the Identify Unauthorized Use Section in the 3.14 System and Information Integrity Policy.

Process Evidence

Identify Unauthorized Use Section
- SharePoint > Govern Docs > Cybersecurity Policy Manual > 3.14 System and Information Integrity Policy

System Baseline Standard
- SharePoint > Govern Docs > Artifacts > System Baseline Standard

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™